This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.0322000

Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation

MIRZA AKHI KHATUN[1,2] *Member, IEEE*, **SANOBER FARHEEN MEMON**[1] *Member, IEEE*, **CIARÁN EISING**[1,2] *Senior Member, IEEE*, **LUBNA LUXMI DHIRANI**[1,2] *Senior Member, IEEE*
[1]Dept. Electronic & Computer Engineering, University of Limerick, Limerick, V94 T9PX, Ireland
[2]SFI CRT Foundations in Data Science, University of Limerick, Limerick, V94 T9PX, Ireland

CORRESPONDING AUTHOR: Mirza Akhi Khatun (e-mail: Mirza.Akhi@ul.ie)

This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number 18/CRT/6049.

ABSTRACT This paper reviews the Internet of Things (IoT) in healthcare, also known as Healthcare-IoT (H-IoT), and its security and privacy challenges. Specifically, smartwatches, blood pressure sensors, and temperature sensors are discussed as IoT devices that pose vulnerabilities. Several risks may arise, such as data breaches, unauthorized access, and potential patient harm. This review explores data security challenges associated with machine learning and H-IoT. Additionally, it emphasizes the importance of monitoring healthcare IoT layers such as perception, network, cloud, and application layers. Detecting and responding to anomalies involve a wide range of cyber threats and attacks, as well as protocols such as Wi-Fi 6, Narrowband Internet of Things (NB-IoT), Bluetooth, ZigBee, LoRa, and 5G New Radio (5G NR). Hence, to protect and mitigate H-IoT devices from the increasing cyber threat landscape, a robust authentication mechanism based on machine learning and deep learning techniques is required. Overall, this paper reviews the security and privacy challenges in healthcare IoT and discusses risk mitigation strategies for building cyber resilience in H-IoT.

INDEX TERMS Healthcare-IoT, Security and Privacy Challenges, Cybersecurity, Threats, Attacks, Anomalies, Machine Learning, Deep Learning, Mitigation Techniques, 5G NR

I. INTRODUCTION

The Internet of Things (IoT) consists of interconnected physical devices exchanging data through sensors, software, and connectivity [1] [2]. In recent years, the healthcare industry has undergone a significant transformation with advances in IoT, cloud, artificial intelligence (AI), and machine learning (ML). According to several experts, the expanding horizon of IoT is expected to improve healthcare. IoT can revolutionize healthcare globally by providing affordable healthcare [3], remote health monitoring [4], wellness management [5], and virtual rehabilitation [6]. Healthcare analytics can provide insight into disease and drug discovery while adding a new dimension [7].

The modern world requires more efficient and timely interventions to combat escalating health issues. While traditional healthcare systems are effective, these systems are often slow and inflexible [8]. The pandemic years have fueled the need for remote and precision healthcare and such objectives could only be achieved by using emerging technologies. Embedding an IoT-enabled architecture in a healthcare ecosystem may facilitate in collecting and processing real-time data from sensors (i.e., body sensors strategically placed on or within a patient's body aiding real-time data collection) [9]. There are different sensors used for different applications such as: motion sensors, flow sensors, and biomedical sensors. However, the ones used for healthcare applications are body sensor networks (BSN) [10]. In a BSN, each sensor is connected to group of sensors forming a network, this configuration enhances data collection and efficiency by integrating IoT body sensors, such as brain wave sensors, temperature sensors, and blood pressure sensors, as depicted in Figure 1. Moreover, the diagram also illustrates how data is stored and transmitted via edge nodes/layer to the cloud for data processing and storage. IoT devices transmit data on millisecond basis and require high reliability, scalability, end-to-end (E2E) latency connectivity networks [1]. To facilitate the required/comprehensive health-monitoring (security and reliability metrics), it is essential to connect the IoT devices with an edge to cloud environment.

As per [11], the need and usage of IoT devices will increase significantly, by 2025 there will be more than 41 billion IoT devices used across the world, having the capacity to

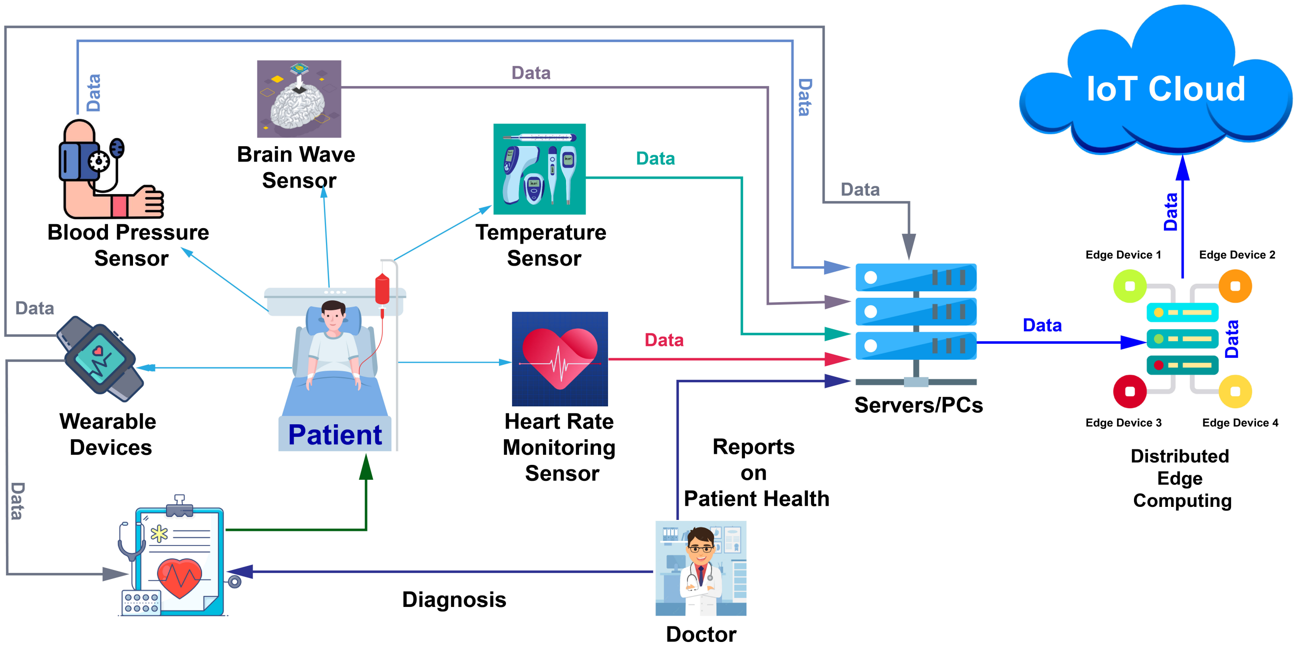

FIGURE 1: **IoT based healthcare architecture**

produce 78 zettabytes of data. Because of its usability, efficiency and applications, these devices have the potential to further advance healthcare by reducing costs, improving patient well-being, and facilitating the efficient delivery of faster diagnostics thereby improving medical services [12]. Furthermore, IoT can provide the migration of patients from traditional methods of healthcare management to new cloud-based systems among other vital innovations [13]. Employing Healthcare-IoT (H-IoT), remote monitoring of patients can save millions of lives and money, while other functions still have a crucial role across healthcare environments [14]. This type of remote monitoring of patients can assist in identifying health issues early on and making treatment plans more personalised. Similarly, IoT can benefit medical management, including medication and instrumental errors, and medication administration—allowing patients to take their medications at the right time and with the correct dosage [15]. Medication error prevention programs can improve patient outcomes and reduce healthcare costs. For example, H-IoT could significantly improve health outcomes and healthcare costs for residents of care homes, who frequently manage multiple medical conditions and take various medications [16].

IoT healthcare frameworks utilize a variety of sophisticated sensors, including diagnostic, sensitive, and preventive sensors, for the implementation of healthcare systems [17]. It has been a primary focus of healthcare researchers over the past few years to find ways to monitor patients remotely and to transmit health reports in real-time to physicians. Researchers have identified several major challenges related to health surveillance systems. The challenges include concerns about data privacy, interoperability issues, data quality issues, and limitations associated with real-time analysis [18] [19]. Patient monitoring concerns can be classified into two categories, static and dynamic monitoring. Smart hospitals use static monitoring systems to keep a record of patient's health status periodically. Moreover, as a static monitoring system, medical staff, including doctors and nurses, manually collect patients' vital signs during specific periods of time. The frequency of manual data collection within hospitals varies based on several factors, such as physicians' workload, working hours, patients' health conditions, and hospital leadership guidance [20]. In contrast to static patient monitoring systems, dynamic patient monitoring systems can be used at home, work, or in the hospital. According to Figure 1, healthcare systems consist of identifying, locating, sensing, and connecting. H-IoT components include emergency medical services, information technology, sensors, lab-on-a-chip technologies, wearable devices, connectivity devices, big data, and cloud computing [21].

Nowadays, smartphones enable rapid task completion by monitoring and collecting regular updates on patients' healthcare data [22]. For instance, an individual can promptly receive notifications when their heart rhythm changes when they wear a wristband linked to their smartphone [23]. Furthermore, IoT provides the healthcare system with the ability to monitor and track community resources in a more efficient and reliable manner [24]. However, H-IoT comes with several risks, including the possibility of privacy leakage during medical data uploading [25]. The risk of patient data disclosure may considerably discourage patients from sharing their medical information because confidentiality is at risk [26]. In healthcare interactions, maintaining confidentiality

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

and credibility are fundamental factors for addressing these risks. Moreover, resolving such security concerns will facilitate seamless deployment and wider adoption of H-IoT.

Over the years, several review papers have been published on the secure healthcare IoT [27]–[38]. There is, however, a noticeable gap in the existing review regarding the security of healthcare IoT, often failing to address all necessary aspects holistically. Most of the discussions focus heavily on the technical aspects of H-IoT devices, diving deep into their specs and applications, skipping over the essential issue of data security. During the discussion of machine learning, the focus is on its potential application in healthcare, instead of exploring how it can enhance security protocols, such as detecting unusual data patterns that may indicate a cybersecurity threat. Security issues related to remote patient monitoring in healthcare IoT have not been discussed in existing reviews either. In [39], the authors analyse the internet of medical things (IoMT) security controls in a sustainable context, but do not address specific issues like remote patient monitoring or the use of artificial intelligence in IoMT security. In [40], IoT and artificial intelligence are explored, and a smart pill bottle case study is presented, however, detailed comparisons of these technologies appear to be lacking, and alternative cybersecurity strategies may not be fully considered. In [41], the authors provide a brief review of wireless body area network-based IoT healthcare systems but do not provide a detailed exploration of real-world implementations and case studies. Furthermore, although the discussion acknowledges security and privacy concerns, it does not provide in-depth solutions or strategies to address identified challenges within IoT healthcare systems. In [42], a detailed review of the Internet of Healthcare Things (IoHT), covering its technologies, applications, and inherent challenges, particularly in terms of privacy and security, is presented in this document. Although it explores many issues, notably privacy and security, it modestly limits its explanations to practical solutions. In [43], the authors discuss the development of 5G technology within the healthcare IoT space, including network slicing, security, and energy efficiency. Despite this, certain topics remain unresolved and require more exploration and innovation. These include data security, efficient resource management, and energy conservation. Healthcare services use large amounts of energy for heating, ventilation, and air conditioning (HVAC) [44]. IoT sensors enable HVAC systems to adjust their settings based on occupancy and usage in real time.

In H-IoT research, secure data access presents a pivotal challenge, particularly in light of healthcare data's regulations and strict policies that apply to protecting patient's identity/confidentiality. Looking at the various ransomware attacks and data breaches [45] that healthcare sectors have suffered in the past affecting millions of patients globally, demonstrates the urgency and need to mitigate these growing cyber risks. This complex research landscape has been reshaped by Cooja simulator, allowing researchers to emulate H-IoT device behaviors without interacting directly with sensitive data. Data collection from healthcare IoT devices was not discussed in previous surveys. In addition, there was a limitation on how malicious data could be collected for anomaly detection by machine learning. This paper reviews the security aspects of H-IoT applications, pinpoints vulnerabilities, and uses ML to suggest solutions, providing an enhanced understanding of the security issues associated with H-IoT that incorporates both practical and theoretical considerations. In addition to highlighting mitigation of H-IoT security challenges, this review also illustrates the use of Cooja simulator tools, which allows a unique perspective to be gained that makes this survey distinctive from those that have previously been conducted.

The aim of this paper is to review current research on artificial intelligence and machine learning techniques that can enhance H-IoT security building cyber resilience within the healthcare infrastructure and enabling it to detect, protect and respond to the novel cyber threats. The paper also covers a broad spectrum of cybersecurity issues from an EU ENISA's 2030 cyber threat landscape foresight [46] perspective including complexities associated with IoT layers. Furthermore, this review outlines promising avenues for future research and highlights the advancements in the field. This review paper highlights the following key contributions:

- Reviews key aspects of cybersecurity, big data, e-health, and cloud computing in healthcare IoT.
- Discusses machine learning techniques such as anomaly detection, device classification, and critical use cases for security enhancement such as intrusion detection, authentication, and access control.
- Highlights the challenges and potential solutions related to H-IoT security, along with future research directions.

Figure 2 presents the structure of this survey paper as follows: section II explains 26 different types of cyber attacks carried out across the four main layers of the H-IoT architecture, section III describes the interaction between emerging technologies, such as machine learning and cloud computing, e-Health system and also discusses the risks associated to Healthcare-IoT, section IV emphasizes risk mitigation strategies, reviews the evolution of cybersecurity challenges in healthcare over the last five years, and provides a comparative analysis of H-IoT attack data-sets, section V explores specific H-IoT layers, including data collection, applications with an emphasis on routing attacks, and network layers, as well as Cooja simulator, section VI focuses on feature extraction, intrusion and event detection, system reliability, and machine learning techniques to enhance cybersecurity, and convolutional neural network in the healthcare IoT, section VII consists of solutions designed for future H-IoT environments, including anomaly detection, security, and privacy, section VIII outlines the future of healthcare IoT technologies, software defined networks, challenges, and mitigation strategies and finally, section IX concludes the paper by discussing future roadmaps and limitations.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

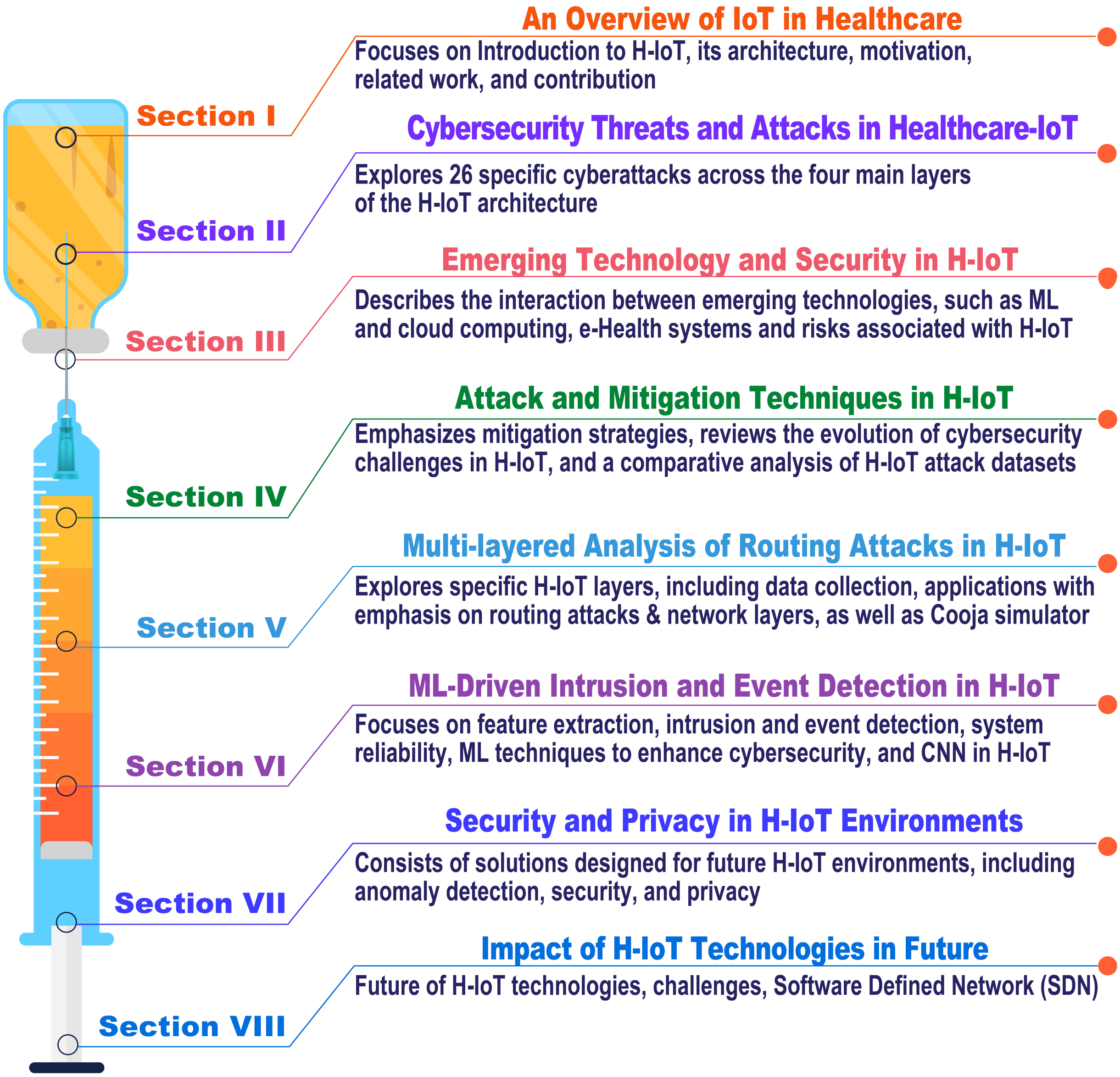
An Overview of IoT in Healthcare
Focuses on Introduction to H-IoT, its architecture, motivation, related work, and contribution
Section I
Cybersecurity Threats and Attacks in Healthcare-IoT
Explores 26 specific cyberattacks across the four main layers of the H-IoT architecture
Section II
Emerging Technology and Security in H-IoT
Describes the interaction between emerging technologies, such as ML and cloud computing, e-Health systems and risks associated with H-IoT
Section III
Attack and Mitigation Techniques in H-IoT
Emphasizes mitigation strategies, reviews the evolution of cybersecurity challenges in H-IoT, and a comparative analysis of H-IoT attack datasets
Section IV
Multi-layered Analysis of Routing Attacks in H-IoT
Explores specific H-IoT layers, including data collection, applications with emphasis on routing attacks & network layers, as well as Cooja simulator
Section V
ML-Driven Intrusion and Event Detection in H-IoT
Focuses on feature extraction, intrusion and event detection, system reliability, ML techniques to enhance cybersecurity, and CNN in H-IoT
Section VI
Security and Privacy in H-IoT Environments
Consists of solutions designed for future H-IoT environments, including anomaly detection, security, and privacy
Section VII
Impact of H-IoT Technologies in Future
Future of H-IoT technologies, challenges, Software Defined Network (SDN)
Section VIII

FIGURE 2: **Structure and outline of the paper**

II. CYBERSECURITY THREATS AND ATTACKS IN HEALTHCARE-IOT

Healthcare Internet of Things (H-IoT) requires a thorough understanding of the technical architecture, which is typically categorized into four layers. These layers include (I) the perception layer, (II) the network layer, (III) the cloud or processing layer, and (IV) the application layer [47]. Cybersecurity threats and attacks emerge at these layers, causing significant challenges (i.e., routing attacks, impersonating, tampering, or data transit attacks at the perception layer, Denial of Service and Distributed Denial of Service (DoS/DDoS) or Man-in-the-Middle (MITM) attacks at the network layer, Cloud-malware injection or Brute-force attacks at the Cloud-IoT Layer and SQL injection or Cross-Site Scripting (XSS) attacks at the application layer) [48]–[54]. This section discusses 26 different cyber attacks and demonstrate their specific mechanisms and impact on the infrastructure. Figure 3 illustrates the details of IoT healthcare layers. It also provides a detailed explanation and insights into the most prevalent threats and attacks occurring at different H-IoT layers.

1) The Perception Layer

This layer can also be termed the "physical layer" or the "sensor layer," as it pertains to the physical devices [55] serves the purpose of sensing and collecting essential information about patients, such as their medical history. IoT healthcare

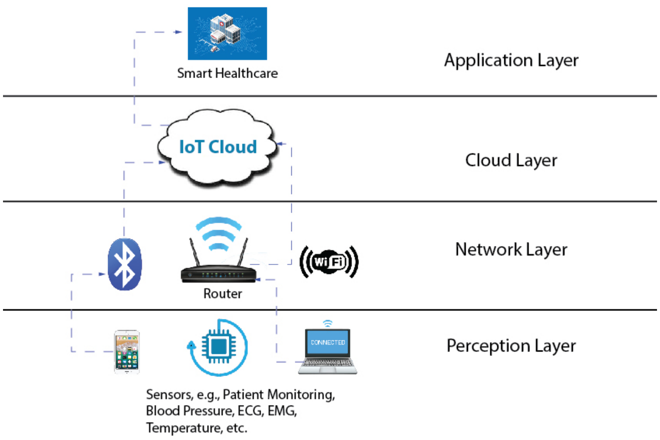

FIGURE 3: **The layers of healthcare IoT**

frameworks enable the interconnection of key stakeholders such as doctors, nurses, technicians, pharmacists, and medical devices as part of the perception layer. A specialist can monitor the data collected by the perception layer in real time over the Internet. There are multiple communication protocols (i.e., Radio Frequency Identification (RFID), Bluetooth Low Energy (BLE), Wireless Sensor Networks (WSNs), Zigbee, and IPv6 over low-power wireless personal area networks (6LoWPAN)) used for collecting and transmitting data from IoT nodes [56]–[59]. This layer is susceptible to multiple attacks that can affect the infrastructure in various ways, as depicted in Figure 4.

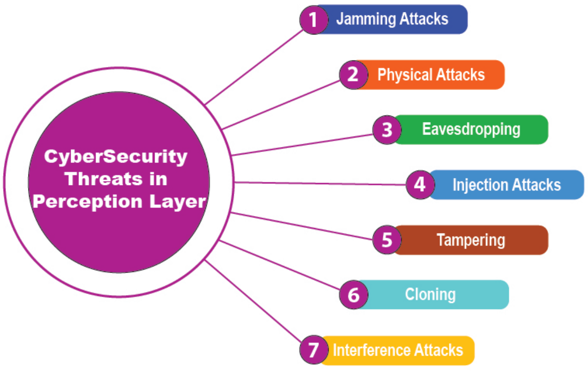

FIGURE 4: **Cybersecurity threats in perception layer**

Here, we summarise each threat in this layer briefly:

- **Physical Attacks:** These types of attacks focus on the IoT architecture's perception layer or physical layer that consists of hardware devices. To carry out an attack at this layer the malicious actor needs to remain closer to network infrastructure or gain unauthorized access to it physically to execute an attack [60]. These exploitations may facilitate the threat actor to tamper with implanted medical devices (i.e. Wi-Fi enabled pacemakers, and insulin pumps.).
- **Eavesdropping:** IoT devices are vulnerable to eavesdropping if such attacks are executed successfully, which gives the malicious actor direct access to retrieve confidential information exchanged between the devices or radio frequency identification (RFID) tags and readers [61] [62] [63]. Eavesdropping attacks may have a variety of malicious intents, such as taking intellectual property, biometrics, and genome data for personal gain or using personally identifiable information/genetic data for espionage [64]. Such types of attacks have been carried out in the past [65].
- **Jamming:** The majority of wireless devices communicate with each other via radio frequency (RF) signals, which can be obstructed by stronger signals. In this scenario, a malicious actor may interrupt and block communications between sensors and receivers leading to an absolute downtime and lack of availability [66] [67]. Jamming stands out as one of the most common attacks carried out at perception layer attack, alongside physical tampering, false data injection, and eavesdropping [68]–[75]. The impact of jamming attacks in H-IoT can be catastrophic as it could disrupt on-going surgeries, medical diagnostics, access to online-systems. In short, it can lead the healthcare facility to an absolute downtime affecting human lives. These types of cyber-attacks have an escalated impact not only on an infrastructure's operational and financial aspects but also on the ethical/social dimensions.
- **RFID Cloning:** These attacks have emerged as a major security concern at the IoT's perception layer as they camouflage themselves in different forms such as RFID cloning and tag cloning. RFID cloning involves replicating and deceiving readers with duplicate tags that simulate similar to the original to gain unauthorized access to information [76] [77]. The concept of tag cloning, however, encompasses the duplication of a variety of tag-based identification systems beyond RFID [78]. These two forms of hacking endanger the integrity of the system and increase risks related to bio-hacking [79].
- **Injection Attacks:** These attacks can occur on various IoT layers, however at the perception layer, it is carried out by injecting a malicious code, and modifying the firmware of an IoT device. IoT infrastructures face the greatest challenge when a single compromised/malicious node can spread across and infect the entire network, causing complete operational disruptions [80]. As per the European Cyber Resilience Act, digital and critical infrastructures must have the ability to detect, protect, respond, mitigate cyber threats, and maintain operational resilience simultaneously [81].
- **Interference:** It can be exploited by intruders by interrupting the network traffic by constantly broadcasting radio waves onto the network for disrupting network

communication [82], or for spreading false information. As per the European Network and Information Security Directive (NIS2-D), the healthcare infrastructures fall under the mandatory infrastructures to comply with the high common level of cyber security across the European jurisdiction [83]. These types of attacks have the potential to spread misinformation and catalyze panic situations.

- **Tampering:** Attackers who manipulate nodes' memory to alter their functionality are called node tamperers. Furthermore, attackers may physically tamper with a device by turning it on and off, restarting it, and stealing its keys, code, and manipulating the data [49] affecting the data integrity of the environment. Due to the misuse of generative AI, adversaries have been orchestrating and executing such attacks more frequently. As per the European General Data Protection Regulation (GDPR) [84], if any sensitive, personally identifiable information (PII) or healthcare data is breached in terms of integrity (data altered, amended, and tampered.) then it is considered as a data breach. As mentioned in the above subsections, the risks associated with the misuse of PII are catastrophic.

Defenses against perception-layer cyber-attacks in IoT are discussed in [85]. However, the approaches may not be effective in mitigating the adversarial and escalating cyber threats occurring due to generative AI.

2) The Network Layer

Data packets are received and processed through this layer by the perception layer. Afterward, the layer transmits the made-trust data to the cloud layer that is immediately above it. The cloud layer's role is to store and share/build trust mechanisms between the smart devices [86] [87]. The network layer can be enabled with different wireless networks (Wi-Fi 6, 5G, Bluetooth, NB-IoT, and LTE.) [88]. As part of the IEEE wireless communication standards, such as 802.11a, 802.11g, 802.11n (Wi-Fi 4), 802.11ac (Wi-Fi 5), 802.11ax (Wi-Fi 6), and 802.11p (for vehicular communications), orthogonal frequency division multiplexing (OFDM) is employed for the effective transmission of data across multiple frequency bands [89]. In the case of IoT devices, high-speed Wi-Fi has recently been recognized as an attractive option due to its compatibility with existing infrastructure [90]. The IEEE 802.11ax, a sixth-generation protocol popularly known as High Efficiency (HE) reports a 30% improvement in throughput over the older IEEE 802.11ac protocol known as very high throughput (VHT) [91]. A 5G-enabled energy-efficient routing protocol (EERP) that uses Wi-Fi 6 makes it easier for medical devices to communicate with one another, while multi-user, multiple input, multiple outputs (MU-MIMO) allows parallel communications [92]. A data-centric protocol prioritizes the transmission of critical health information, and content-centric networking (CCN) improves the efficiency of the distribution of healthcare information between IoT devices [93].

The vulnerability to DDoS attacks has increased dramatically with the advent of 5G. A distributed network architecture with multiple remote edge computing sites is essential for achieving low latency, which is critical for vehicle-to-vehicle communication. Additionally, the dense network of connected devices, open-source applications, and additional points of access all contribute to increasing "attack surfaces". Furthermore, higher wireless speeds dramatically increase the impact of DDoS attacks on the network since each device can transmit an order of magnitude higher attack throughput to the network (at MECs and at the core). As mentioned, this effect is amplified by the plurality of IoT devices, which is expected in 5G, due to the vulnerability of IoT devices to cyberattacks [94]. Figure 5 illustrates seven types of attacks that are most encountered at this layer. The following discussion highlights key attacks in the network layer of the IoT:

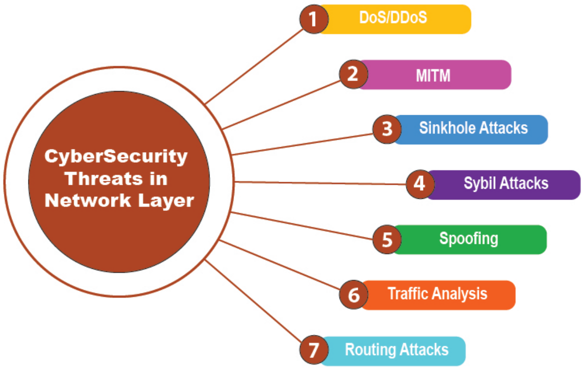

FIGURE 5: **Cybersecurity threats in network layer**

- **Dos/DDoS Attacks:** In smart ecosystems, denial of service (DoS) and distributed denial of service (DDoS) attacks are prevalent [95]. During a DoS attack, a hacker attempts to consume legitimate network resources or bandwidth. This attack is referred to as a DDoS when it originates from multiple compromised nodes [96] and falls into different categories such as traffic/fragmentation attack, bandwidth attack, and application attack) [97]. Wireless and wired networks are critical to DDoS attacks, which target the network layer [98]. Flooding the Internet control message protocol (ICMP) and user datagram protocol (UDP) with excessive data leading to delays, resource consumption, potential system crashes, and ultimately disrupts services are common methods for executing these attacks [99] [100]. These attacks would lead to absolute downtime and operational disruption.
- **Routing Attacks:** Throughout the Internet of Things, IPv6 is widely used, especially in wireless sensor networks (WSNs). IPv6-centric WSNs are particularly vulnerable to routing attacks. Furthermore, WSN sensors are frequently constrained by memory limitations, nar-

row bandwidths, and energy consumption [48]. These attacks are generally carried out at the Internet Service Provider's level and there it is mandatory for Information and Communication Technology (ICT) service providers to be NIS2-D compliant [101]. Detailed information about routing attacks can be found in section V-C.

- **Traffic Analysis:** Network traffic is analyzed for detecting and monitoring malicious behavior and anomalies. Depending on the network traffic, routers manage data packets. Each router is equipped with a certain amount of capacity. Clogging or unusually high traffic may indicate traffic analysis or even a denial-of-service attack [102]. Malicious actors at times observe the traffic for guessing passwords, by analyzing the packets sent during each keystroke and assessing the duration between them. By using such a pattern, they can reconstruct the users' passwords.
- **Spoofing Attacks:** Several types of spoofing are possible, such as email, URL, and frame spoofing. It is, however, MAC spoofing or IP address spoofing that is most widespread [103]. IoT uses the MAC address to authenticate wireless networks at the data link layer. Spoofing attacks occur when malicious entities imitate legitimate users' MAC addresses to gain network access illegally affecting the data confidentiality and integrity of the environment [104]. Lack of data confidentiality means unauthorized/malicious actors may know the contents of data, whereas lack of integrity means the data may have been amended, altered, tampered or discarded. As per GDPR lack of the security (Confidentiality, Integrity, and availability) metrics and controls is considered a GDPR breach.
- **Sybil Attacks:** IoT devices are vulnerable to the Sybil attack [105] [106]. In this attack, legitimate nodes are impersonated by malware to redirect traffic towards malicious ones. An individual node can appear in multiple locations simultaneously or impersonate several others [107]. During this attack, a malicious node claims to have multiple identities. Due to their ability to control the flow of information within a network, these types of attacks affect data integrity and resource allocation.
- **Sinkhole Attacks:** In sinkhole attacks, traffic is redirected or discarded by the attacker, preventing the base station from receiving full data transmission. In this attack, misleading routing details are spread from one node to another, resulting in energy drain and reduced network durability. The depletion of energy is particularly damaging to wireless sensor networks (WSNs) [108]. These types of attacks affect the integrity, availability, and reliability of data in a network.
- **Man-in-the-middle (MITM) Attacks:** Man-in-the-middle attacks involve intercepting communications between two devices by an attacker [51]. The main target of MITM attacks is the confidential details of users [53]. Malicious actors exploit existing or new vulnerabilities in IoT systems to carry out this attack. An example would be a temperature reading of a sensor or malfunctioning of a device enabling hackers to steal sensitive information [109].

3) The Cloud Layer

The cloud allows for convenient and secure backup and preservation of confidential health information, and its sharing between authorized parties (such as doctors, insurance providers, medical staff, and pharmacies) is convenient. Similarly, independent and public healthcare providers can maintain confidential data online and share it with trusted colleagues to improve the quality of treatment. These protocols include transmission control protocol (TCP), user datagram protocol (UDP) [110], and protocols for data analysis, prediction, and machine learning [111]. Figure 6 depicts several distinct threats related to cloud layers. These specific vulnerabilities are explained in the following sections:

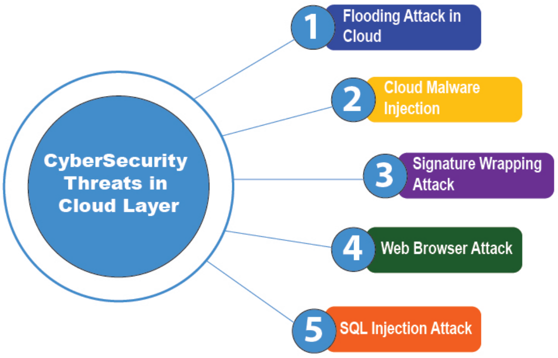
CyberSecurity Threats in Cloud Layer
1 Flooding Attack in Cloud
2 Cloud Malware Injection
3 Signature Wrapping Attack
4 Web Browser Attack
5 SQL Injection Attack

FIGURE 6: **Cybersecurity threats in cloud layer**

- **Flooding Attacks:** Flooding attacks are a type of DDoS attack that disrupt services by overloading the servers with enormous traffic from compromised computers. During these attacks, excessive messages are sent to servers, which causes legitimate users to be denied access to the Internet [112]. In the cloud environment, attackers often rely on sophisticated methods to take advantage of its inherent scalability and flexibility [113].
- **Web Browser Attacks:** Throughout the modern digital era, web browsers have become integral tools that allow users to access a variety of online services and connect to the vast internet. Nowadays, browsers are a crucial component of almost every computer. Nevertheless, browsers are not immune from vulnerabilities [114], [115]. As a result of these vulnerabilities, attackers often gain access to a victim's computer, steal PII, corrupt files, or use the hacked machine to attack others, potentially becoming a part of a botnet [116].
- **Signature Wrapping Attacks:** Cloud infrastructure attacks may provide attackers with root-level access to

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

systems, without the need to target the cloud environment directly [117]. The authentication systems of cloud interfaces are vulnerable to advanced cross-site scripting (XSS) methods and signature wrapping [118]. In addition to manipulating virtual machine operations and password resets, signature-wrapping attacks are also known as XML signature-wrapping attacks [119]. In contrast, attackers can steal login credentials by exploiting the XSS vulnerability [120].

- **Cloud Malware Injection Attacks:** Attackers perform malware injections by inserting malicious code or services into a network, appearing as if these components were legitimate components already present [54]. As a result of this attack, users are often deceived into downloading software or opening malicious emails. This type of attack is sometimes known as driven by downloading or meta-data spoofing. An attacker may trick users into downloading harmful software by creating a deceptive environment. In the aftermath of such an attack, users may have limited access to their systems, while attackers may be able to execute malicious activities in the cloud and gain unauthorized control [121].
- **Structured Query Language (SQL) Injection Attacks:** Cloud computing often exposes web services to various security threats due to their inherent Internet accessibility. SQL injection is one of the most widespread risks [52]. SQL injection attacks involve manipulating SQL queries to accomplish malicious objectives. Consequently, sensitive data may be modified unauthorized, confidential details may be accessed, or even the server may crash as a result of such manipulation [122].

4) Application Layer

Within the IoT architecture, the application layer resides at the top level. This layer provides the user interface, which includes services such as healthcare, smart homes, and connected cars [123] [124]. It recognizes spam and filters out the malicious content [125].

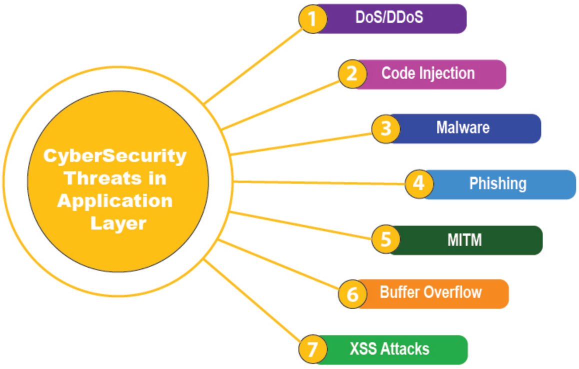

FIGURE 7: **Cybersecurity threats in application layer**

Figure 7 illustrates IoT applications' primary security threats. The following sections delve into the application layer vulnerabilities:

- **DoS/DDoS Attacks:** DDoS attacks are carried out by a group of compromised computers operating from multiple locations that flood a particular target with traffic. In this attack, the primary goal is to overwhelm and render unavailable a server, website, or online service [126] [127]. In the event of a DDoS attack, IoT devices such as smart appliances, healthcare monitors, and industrial sensors can be rendered useless [128]. In addition to affecting their immediate functionality, disruptions can jeopardize critical operations they oversee, like monitoring patient health or maintaining optimal building conditions [129].
- **Phishing Attacks:** Phishers can use compromised devices such as smartphones, appliances, and smart cars to conduct phishing attacks at the application layer. Through this method, attackers impersonate legitimate devices and send messages that appear to be authentic. A malicious attacker can then manipulate or obtain credentials to authenticate or identify, which can then be used for criminal purposes [130]. For example, the Irish HSE Conti Cyber attack [131], which was initially a phishing attack, soon escalated to a ransomware attack after an employee accidentally clicked on the malicious email disrupting the healthcare facility operations and IT outages across the country for days. However, it took 4 months for the Irish HSE to completely recover from the aftermath. This is why it is mandatory to build cyber resilience within such infrastructures.
- **Buffer Overflow Attacks:** Buffers hold data while it is transferred from one location to another. In buffer overflows, data exceeds the buffer's storage capacity. As a result, the application may crash, memory access errors may occur, and results may be incorrect. Memory overwrite vulnerabilities can be exploited by attackers. It can affect execution paths, leak confidential information, and corrupt files [132]. Legacy systems are most vulnerable to these types of attacks as they have limited memory [1].
- **Malware:** A malware attack attempts to use a malicious program to commit an offense with IoT applications, and recently, many malicious programs have been released to attack IoT devices, including rootkits, spyware, and adware [133]. [1] [134] discuss different types of malware and their impact on the national security (i.e., Red October), social (transportation, communications, energy, and water sectors), financial (BaFin) [135] and economic domains (manufacturing, fintech) affecting human lives [136].
- **Cross-site Scripting (XSS) Attacks:** In cross-site scripting (XSS) attacks, harmful code is embedded into an authentic and trusted website [137]. An attacker can alter the content of an application through this poten-

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

tially dangerous intrusion [138]. Due to the inability of the targeted browser to distinguish between genuine and malicious code, the infected code is executed. Consequently, this malicious code is capable of accessing cookies, session identifiers, or other confidential information. In addition, the attacker can control the device directly, sending users to malicious websites or causing direct damage to the device.

- **Unauthorised Scripts Attacks:** These attacks occur when unwanted or malicious scripts are executed without the user's consent. In contrast to XSS attacks, which target the user's browser, unauthorized scripts can run anywhere in the system or application. Data breaches, system malfunctions, or other vulnerabilities may result from this [139].
- **Code Injection Attacks:** Code injection attacks that use SQL injection break the data-code isolation rule by inserting malicious SQL codes into input fields [50]. In web forms, Uniform Resource Locators (URLs), or page requests, attackers can embed these malicious SQL commands. In the absence of proper filters, a web application may process these harmful commands incorrectly. As a result, unwanted access to the database can occur [140].

III. EMERGING TECHNOLOGY AND SECURITY IN HEALTHCARE IOT

Technological advancements, including the internet of things, machine learning, and cloud computing, are gradually reshaping the Healthcare-IoT. This development creates innovative healthcare solutions, but also challenges, particularly when it comes to data security. AI and machine learning have made great progress in cyber security domains such as intrusion detection and malware mitigation [141]. This section explores the conjunction of machine learning and cloud technologies, scrutinizing emerging trends and attendant security considerations within e-health applications, with the objective of establishing a secure and innovative framework for H-IoT implementations. This section explores the connections between machine learning and cloud technologies within e-health, navigating through emerging trends and assessing related security concerns. Deep learning (DL) and machine learning (ML) are increasingly integral to mitigating cyber threats, however, how these technologies impact e-health is a crucial issue [142]. Providing a secure and innovative foundation for H-IoT implementations is the goal of this section.

A. MACHINE LEARNING WITH CLOUD COMPUTING

Researchers all over the world have applied machine learning to a variety of applications and domains [143]. Recently, ML has drawn the attention of healthcare IoT researchers [144]. In the context of H-IoT, machine learning is beneficial for remote monitoring and real-time treatment of diseases [19] [145]. ML algorithms such as support vector machines (SVMs), Decision Trees, random forests, and artificial neural networks (ANNs) can analyze huge volumes of medical data collected by healthcare-related smart devices, including vital signs and medical histories [146]. In this process, ML techniques are applied to analyze massive datasets to find patterns and generate insights that may assist clinical decisions, improve patient outcomes, and reduce healthcare expenditures. Cloud computing, however, provides computing power and storage resources for healthcare IoT to support machine learning based on big data collected from IoT devices [147]. ML algorithms utilize the cloud to process and analyze data and provide a secure and scalable computing environment [148].

Forum et al. [149] developed a Health-Cloud platform by using machine learning and cloud computing to track the condition of patients suffering from heart-related diseases. Moreover, the researchers built a live data analysis iOS App using Google Cloud Firebase.

Abdelaziz et al. [150] investigate the use of IoT and cloud computing in healthcare to predict chronic kidney illness in a city of the future. IoT devices transmit chronic kidney disease (CKD) data to cloud storage, improving prediction accuracy. The hybrid model, which combines linear regression and neural networks, predicts CKD with 97.8% accuracy. Cloud IoT offers tremendous potential in healthcare services, benefiting patients and smart city stakeholders.

B. ELECTRONIC-HEALTH (E-HEALTH) SYSTEMS

The exchange of health records between doctors and patients is now conducted largely electronically, using technology to transfer patient data efficiently and facilitate communications between doctors and their patients. As illustrated in Figure 8, e-health application systems can solve a number of problems associated with traditional healthcare systems, including online appointments, medical evidence, information technology, communication, e-prescribing, medical history, reminders, payment management, and lab analysis. e-healthcare services can enhance patient data management and health information management [151]. As a result, patients can access their medical records online, receive remote consultations, and use mobile health applications to manage their health, which increases accessibility and empowers patients.

Maksimović et al. [152] describe the gradual adoption of e-health platforms, as primarily due to infrastructure and political restrictions. Despite these challenges, e-health and IoT convergence is progressing. However, there are hurdles like consistency, security, and interoperability in IoT integration. Privacy concerns and regulations further complicate the adoption of large-scale technologies. The paper highlights the influence of IoT in e-health and outlines these crucial challenges, emphasizing the importance of overcoming barriers to implementation. Zhang et al. [153] explore how fifth-generation (5G) technology can revolutionize e-health. While 5G promises reliable access to e-health, current efforts are not sufficient. In this paper, the authors also discuss technological aspects, practical use cases, and research trends and challenges in advancing 5G e-health.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

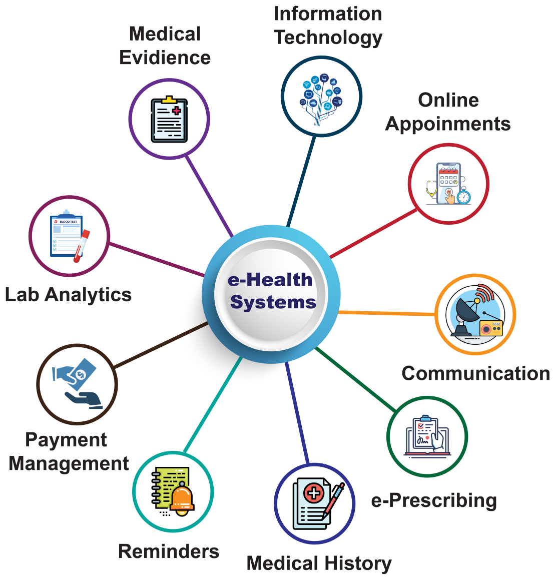

FIGURE 8: **e-Health Systems**

C. BIG DATA IN HEALTHCARE-IOT

IoT networks generate enormous amounts of data at every moment. Therefore, manipulating so many datasets requires considerable technical expertise. IoT architecture and machine learning techniques boost big data capacity, and advanced deep learning (DL) models are essential [154]. By utilizing big data analytics, smart healthcare systems have transformed mathematical modeling with data collection dynamically. Besides collecting and storing data, big data is also about empowering machines to think and act like humans to simplify complex tasks [155] [156]. Wearable sensors continuously collect data, such as sleep patterns, exercise levels, walking distances, heart rates, etc. The latest IoT sensors can also monitor heart rate, blood sugar levels, and pulse. A major benefit of big data for the medical industry is that it could reduce the costs of accommodations, travel time, and transportation delays. In addition, big data analytics have improved healthcare facilities and enabled patients to recover at home [157]. H-IoT devices can also decrease medical expenses by reducing personnel and transport costs with big data [158] [159].

Hiba et al. [160] developed a real-time disease prediction platform that enhances patient care and reduces healthcare costs with the aid of a Big Data platform. It helps users make better decisions in real time, resulting in improved health and safety. Heart attacks, obesity, and miscarriages can be detected using this approach. Long-term treatment and hospitalization costs can be reduced by early detection and accurate prediction of health problems.

Sasubilli et al. [161] utilize machine learning and big data to analyze the use of electronic health record applications in neuro- and cardiac-related fields. In healthcare architecture, the integration of machine learning approaches and big data frameworks enhances data management, while improving patient care as well. Advanced technologies enable more precise diagnostics, personalized treatment plans, and better outcomes, elevating patient care standards.

D. RISK CATEGORIES IN HEALTHCARE-IOT

Healthcare IoT brings multiple risks associated with medical devices integrated with advanced technologies. Data privacy, device vulnerability, service reliability, and ethical issues are all included in these risks. Both security and user trust depend on addressing these issues.

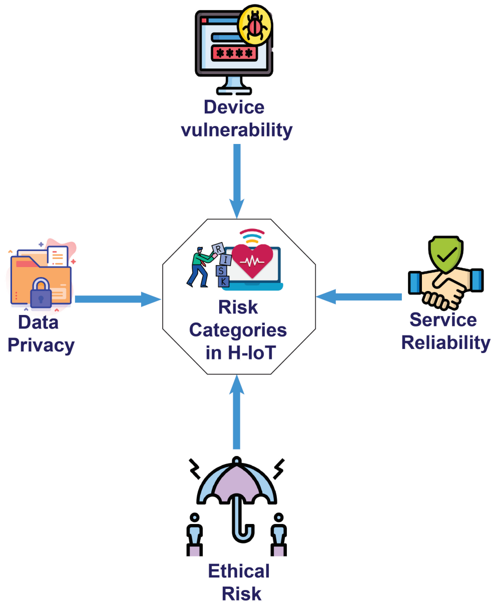

FIGURE 9: **Risk categories in H-IoT**

As depicted in Figure 9, these risk categories apply to the H-IoT industry. The following sections discuss each risk category and its impact within the context of H-IoT:

- **Data Privacy Risk:** During the COVID-19 pandemic, several countries reduced their data privacy guidelines as part of their emergency response [162]. Per the EU General Data Protection Regulation, implementing data security, governance, risk, and control metrics has been mandatory since the regulation was enacted in 2018, The regulation also enabled and improved the cyber security posture of organizations working across Europe in comparison to other countries/jurisdictions and this is why Europe suffered lesser data breaches in comparison to the rest of the work. In the context of digitally enabled precision healthcare, securing systems and enforcing strong data controls are essential to mitigate risks associated with emerging technologies [163], this would mean enabling end-to-end data (data-in-use, data-in-transit, and data-in-store) security, encrypting, anonymizing and pseudonymizing it, to mitigate the risks of data breach.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

Whenever adversaries are able to steal data that has been encrypted, anonymized, and pseudonymized, the data will have no value to the hackers [134].

- **Device Vulnerability Risk:** IoT has many security vulnerabilities, especially in the H-IoT space because these devices would be manufactured by different suppliers who would not have considered security by design and privacy-by-design metrics leading to unencrypted network services, inadequate password protocols, and user interface credentials. These issues have been identified as serious security lapses in 70% of H-IoT devices [164]. In addition, 90% of these devices collect personal data [165], illustrating the complexity and diversity of this issue. Healthcare sectors across the world are particularly vulnerable to cyber threats owing to their diverse operating environments and intricate regulatory frameworks. However, ENISA has passed new cybersecurity standards and regulations to combat supply chain risks, digital services risks, digital market risks, and third-party risks [134].
- **Service Reliability Risk:** In healthcare IoT, service reliability risks refer to service interruptions or failures, which can cause critical delays or data loss. This is a major concern for emergency response and ongoing health monitoring. Healthcare IoT services require effective interference mitigation and optimization of 5G networks. In order to fully benefit from 5G and IoT, these steps will enhance reliability and efficiency [166]. With the deployment of 5G and Beyond 5G (B5G), service interruptions, data loss, and seamless communications between multiple devices will be prevented in healthcare IoT or the Internet of Medical Things (IoMT) [167]. The ability to transmit real-time, accurate patient data to medical personnel through 5G and B5G is especially crucial in medical emergencies [168].
- **Ethical Risk:** A potential ethical risk associated with IoT devices is that of unethical actions [169]. There is an example from the automotive industry that serves as a cautionary tale, even though it isn't directly related to Healthcare IoT. In violation of the Clean Air Act, Volkswagen developed and installed software to manipulate diesel emissions tests [170]. Reputational and financial damages resulted from this breach of ethics. When it comes to H-IoT, where patients' health and well-being are at risk, cyber ethical breaches such as harm to privacy, harm to property, and misuse of technical resources [134] can be detrimental [171].

IV. ATTACK AND MITIGATION TECHNIQUES IN H-IOT

With the use of cutting-edge technologies in the healthcare industry, the security and privacy risks have drastically increased [134]. As per [172] in 2022, more than 200 cyber attacks were carried out across healthcare organizations in the world on a daily basis by malicious actors, impacting millions of people worldwide. The number of cyber attacks on H-IoT have increased by an alarming 74% in 2023 [173]. The demystification of cyber threats and attack scenarios is crucial to preventing these escalating risks. Therefore, this section explores the cybersecurity landscape of healthcare IoT. Table 1 surveys cybersecurity challenges within the healthcare sector over the last five years. Furthermore, this section discusses attack datasets for detecting and mitigating anomalies in H-IoT environments, as well as threats, potential impacts, and mitigation strategies.

A. MITIGATION TECHNIQUES

This section presents findings on mitigation strategies employed in prior research to mitigate cyber security threats associated with IoT in healthcare. Figure 10 illustrates the strategies for access control, encryption, authentication, AI/ML, blockchain, digital signatures, and firewalls/antivirus. Healthcare IoT solutions also integrate modern technologies based on artificial intelligence and deep learning. For instance, Al-Garadi et al. [174] described that machine learning models have been incorporated into security solutions to identify vulnerabilities and attack surfaces. Qiu et al. [175] explore the integration of healthcare and smart cities, enhancing health practices in countries around the world. Blockchain technology addresses the security concerns raised by this integration, thereby ensuring the confidentiality of patient data. The authors discussed the benefits and drawbacks of each of the models used in the research at different IoT layers.

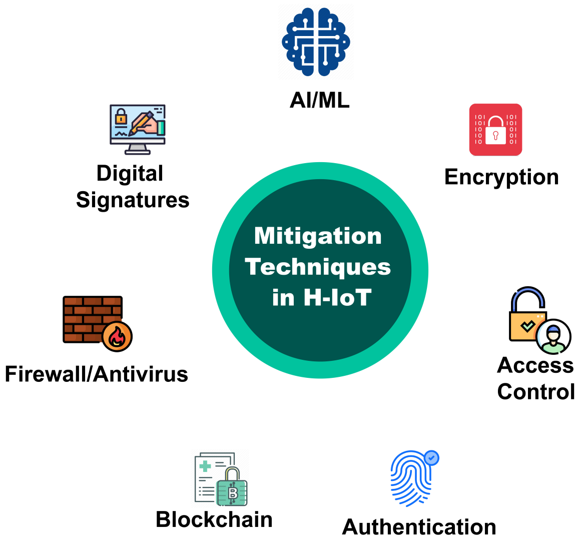

FIGURE 10: **Mitigation techniques in H-IoT**

B. COMPARATIVE REVIEW OF H-IOT ATTACK DATASETS

Datasets are crucial in identifying and mitigating anomalies in the ever-expanding world of the IoT in healthcare, industry, and general applications. H-IoT attack datasets are reviewed in this subsection, including simulations and real-world data from healthcare IoT sensors. In the constantly evolving area

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

of healthcare IoT, these datasets serve as essential tools for research [176]. In a similar way, machine learning applications require high-quality healthcare data, and exact labeling improves its accuracy [177]–[179]. Table 2 provides a detailed overview of datasets, attacks, mitigation techniques, benefits, and limitations.

Key Publications	Area	Security and Privacy Issues
Garcia-Perez et al. [180] (2023)	H-IoT	The paper highlights the lack of cyber risk awareness, management, and security risks related to emerging technologies.
Cartwright et al. [181] (2023)	IoMT, COVID-19	Security gaps in Protected Health Information (PHI), Internet of Medical Things (IoMT) challenges, COVID-19 amplification, and funding shortages.
Javaid et al. [182] (2023)	H-IoT, Data Security	Risks identified in the paper include ransomware attacks, unauthorized access to patient information, device vulnerabilities, and healthcare data source complexity.
Kumar et al. [183] (2023)	H-IoT	H-IoT devices face various security threats and scalability and latency challenges.
Sharma et al. [184] (2023)	DL, Cyber-attacks, Intrusion Detection System (IDS), Healthcare	A Deep Learning-based IDS detecting cyberattacks achieves 84% accuracy, increasing to 91% with Generative Adversarial Networks(GANs) balanced data.
Khatkar et al. [185] (2023)	DL, Intrusion Detection, Healthcare	For intrusion detection in healthcare, evaluating a DL-based Long Short-Term Memory (LSTM) algorithm against a Decision Tree, SVM, K-nearest neighbors (KNN).
Ksibi et al. [186] (2023)	IoMT, Cybersecurity, ML, Risk Assessment	Analyzes the security risks in the Internet of Medical Things (IoMT) using ML algorithms for anomaly detection and introducing of a new model of risk assessment.
Bouabida et al. [187] (2022)	Pandemic-driven, patient data risks	A significant concern raised by the COVID-19 crisis is the security and confidentiality of patient data.
Wang et al. [188] (2019)	Big Data, H-IoT	An Analysis of Big Data analytics in healthcare is presented, including its advantages and challenges.
Coventry et al. [189] (2018)	Cybersecurity in Healthcare	Due to cybercrime risks, healthcare technology needs a holistic security program.

TABLE 1: Cybersecurity challenges in H-IoT

V. MULTI-LAYERED ANALYSIS OF ROUTING ATTACKS IN H-IOT

This section focuses on routing attacks in the healthcare IoT domain, reviewing key components sequentially. The first step is to discuss the vital process of collecting health-related data in the layer for medical data collection. Following the collection of raw medical data, the medical application layer transforms it into meaningful healthcare services. Next, this section discusses the role and vulnerabilities of the routing and network layers in the context of routing attacks. The next step is to emphasize that the medical application layer is crucial to translating data into actionable insights. In addition, this section discusses the role of the COOJA simulator in collecting data and generating datasets in the healthcare IoT environment.

A. MEDICAL DATA COLLECTION LAYER

Healthcare data is collected by smart healthcare sensors, such as devices for tracking brain activity and blood pressure. A doctor can track the progress of an elderly patient by using IoT devices that record every detail and activity. Staff members and nurses who care for elderly patients receive information. Healthcare IoT integrates healthcare devices at home for disabilities. Therefore, patients' cases may be followed and monitored at any time by the doctor. Despite this, the data generated and collected are susceptible to various threats. As a result of the attacks, hackers can gain complete command and control (C&C) disrupting the devices [1]. These attacks can drain sensors' power, causing them to fail or run afoul of the entire IoT network in the healthcare industry. Medical data collection includes collecting, analyzing, and monitoring data, as shown in Figure 11.

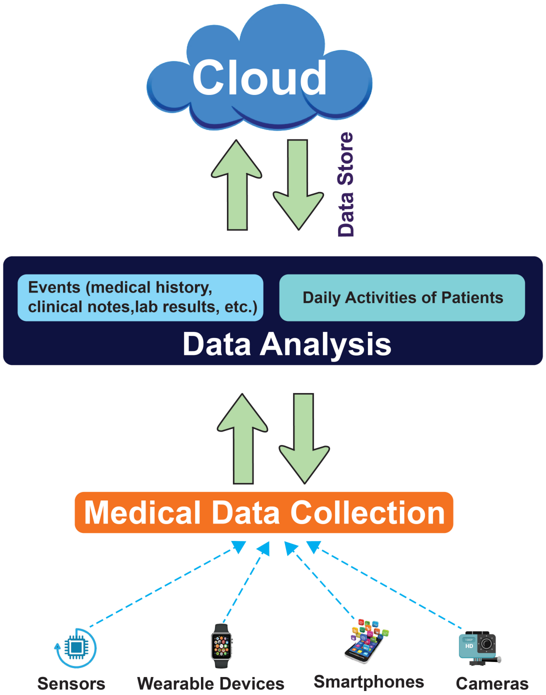

FIGURE 11: **Data collection layers in healthcare**

As a starting point, several types of devices are used for collecting data within the medical data collection layer. These devices include sensors, cell phones, wearable devices, and cameras, among other things. The second phase involves data analysis, which analyzes every event and activity of an

Reference	Techniques Used	Targeted Attacks	Key Benefits	Limitations	Dataset Employed
Wagan et al. [190] (2023)	Dynamic Fuzzy C-Means clustering, Customized Bi-LSTM technique.	Botnet-based DDoS, Zero-day network attacks.	- Separates attacks from regular IoMT data. - Securely handles medical data. - Analyzes attack patterns in IoMT.	- Inequity in the model. - Model decisions are not comprehensible. - Possibility of corruption of data.	WUSTL-EHMS-2020 is a dataset of heart disease with 36 attributes and 18940 instances developed with the Enhanced Healthcare Monitoring System (EHMS).
Thulasi et al. [191] (2023)	Multi Step Convolutional neural network Stacked Long short term memory architecture (MSCSL), Light Spectrum Optimizer (LSO) for optimizing MSCSL's hyperparameters.	Port scans, Brute force, DoS attacks.	- Data adaptability improved. - Reduced computational complexity. - High precision, accuracy.	- Privacy issues are not addressed. - Not optimized for multicloud/fog based dynamic. environments with multiple devices.	Supervisory Control and Data Acquisition International Electrotechnical Commission (SCADA IEC 60870-5-104) datasets.
Gupta et al. [192] (2022)	Tree classifier-based network intrusion detection model.	Man in the Middle Attack (Data Alteration and Data Spoofing).	- Reduced input data dimension effectively. - Accelerates anomaly detection.	- The dataset only consists of Data Alteration and Data Spoofing attacks. - Tested on a restricted network. - Difficulties in formulating IoMT security design.	A combined network flow and biometrics dataset by [193]
Saif et al. [194] (2022)	Hybrid Intelligent Intrusion Detection System (HIIDS), known-Nearest Neighbor (kNN) and Decision Tree (DT), Hybrid approach for feature selection and classification.	Cyber-attacks such as Ipsweep, Portsweep, Smurf, and Brute Force target cloud servers containing Electronic Health Records (EHR).	- Malicious traffic detection and prevention in H-IoT applications. - Metaheuristic algorithms for feature selection reduced computation costs. - Hybrid approach improves intrusion detection accuracy.	- Uncertain performance under high-traffic or larger datasets. - The comparison is limited to Decision Tree and kNN models. There are several ML algorithms, and some are preferable for particular types of data or threats than others.	The NSL-kDD dataset contains 41 features with 125,973 samples.
Ray et al. [195] (2022)	A novel DDoS detection algorithm, DDoS preventive algorithms.	Distributed Denial of Services (DDoS) attack.	- Effectively detect DDoS attacks. - A system that restricts access to attackers.	- Other DDoS attacks may not be suitable for this approach. - If nodes do not filter false data, the system may become complex.	Cloud-based simulated dataset.
Kumar et al. [196] (2022)	A fuzzy min-max neural network (FMMNN) based on fuzzy sets, Supervised algorithm for classification.	DoS, Remote to Local (R2L), User to Root (U2R).	- Nonlinear class boundaries can be learned in one pass. - Detects intrusions more effectively. - Reduced error rate.	- The training time of the FMMNN algorithm needs to be optimized.	NSL-KDD dataset.
RM et al. [197] (2020)	ML algorithms (Supervised & unsupervised), Deep Neural Network (DNN).	Replay, Man-in-the-middle, Impersonation, Privileged-insider, Remote hijacking, Password guessing, DoS attacks, Malware attacks.	- Classification & detection (network/host). - Detects anomalies reliably. - DNN compared to other ML algorithms.	- Unpredictable attacks. - Scalability issues. - Network behavior changes rapidly. - Evolving attacks quickly.	Kaggle benchmark dataset for intrusion detection.

TABLE 2: Comparative analysis of techniques and targeted attacks in published research

elderly patient. A secure server then processes and stores the data. Monitoring healthcare data remotely and automatically recording it includes a patient's medical history and status [198].

B. MEDICAL APPLICATION LAYER

Data processing, storage, and user interfaces are handled by the traditional application layer in IoT environments. On the other hand, the medical application layer is uniquely designed for handling healthcare-related applications, data, and services, ensuring it follows the highest regulations in accordance with the EU General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA) [84] [199] while processing United States healthcare data. This layer presents unique challenges and complexities. For example include Electronic Health Records (EHRs) for patient data, remote consultation platforms, real-time monitoring systems, medical resources, medical care, and diagnosis personnel. Moreover, medical records are processed, organized, and maintained by the medical application layer. This layer ensures that patients' data is authentic, secure, private, and reliable when transmitted over the communication system [200]. Numerous application layer protocols exist, including message queuing telemetry transport (MQTT), hypertext transfer protocol (HTPP), WebSockets, RESTful, secure-MQTT, and constrained application protocol (CoAP) [201]. Choosing the appropriate protocol for H-IoT depends on its application [202].

C. ROUTING ATTACK AND NETWORK LAYER

The network layer defines paths for the routing of data over the network. It has been demonstrated that low-power wireless networks with multiple hops are susceptible to a wide range of attacks, with routing attacks emerging as one of the most significant threats in the healthcare IoT environment [203]. There are many types of routing attacks, including selective forwarding attacks and replay attacks [204]. In the selective forwarding attack, control packets are deliberately forwarded within the Routing Protocol for low-power and lossy networks (RPL) while data packets are dropped. In conjunction with sinkhole attacks, this strategy can disrupt established routing paths and lead to severe consequences for the network [205]. A replay attack entails capturing and re-transmitting packets captured from nearby nodes by an unauthorized node or attacker [206]. The purpose of these attacks is to manipulate or obstruct the transmission of data packets in order to impair the integrity of the network [207]. Furthermore, rank and wormhole attacks are susceptible to IoT routing protocols due to their lightweight nature and limited computational resources. Using these attacks, IoT infrastructures can be devastated by attacks targeting control messages and resources [208].

Routing and network layers receive data sent by medical data collection layers. These layers use protocols such as Wi-Fi 6, Narrowband Internet of Things (NB-IoT), Bluetooth, IPv6 over low-power wireless personal area networks (6LoWPAN), RPL, WiMAX, ZigBee, Sigfox, LoRa, and 5G NR (New Radio) to transmit data to the medical application layer [209] [210] [211]. This setup requires the analysis of routing attacks, potentially compromising confidentiality and accessibility of medical data. To ensure reliable and secure data transmission, protocol configurations designed for power-efficient and unstable networks should be carefully reviewed for vulnerability to various routing attacks [212]. Following the discussion of routing attacks and network layers, this section explores the use of machine learning to detect such cyber threats in H-IoT environments.

As highlighted by [213], healthcare IoT networks are vulnerable to routing attacks, such as sinkholes and wormholes. The authors have introduced various ways to detect such attacks. As a result of the limited resources of devices used in H-IoT, intrusion detection systems cannot be used. By using machine learning and deep learning, the proposed method efficiently detected and handled network attacks while taking device limitations into consideration.

According to [214], especially in e-health applications, protecting sensitive patient data from routing attacks and security threats is pivotal in 5G-IoT. Cloud-based e-health data is at risk of various cyber-threats (i.e, ransomware, loss of privacy, and digital identity fraud.) and attacks mentioned in section II. CNN-DMA is a deep learning model that effectively detects malware attacks by using a type of network known as a Convolutions Neural Network (CNN). The e-health apps enabled with 5G-IoT, deep learning models such as CNN-DMA are useful for ensuring data safety and system security against cyber-attacks. The deep learning models can be trained directly from original data, such as images and text [215]. Therefore, raw data does not need to be preprocessed before being used for learning. Moreover, deep learning algorithms enable seamless execution of security protocols without consuming significant computing resources, which is one of the major benefits of 5G cybersecurity [216].

In light of the delicate nature of healthcare data, it is imperative to enhance security within H-IoT's network layers. By leveraging machine learning and deep learning, as shown in the examples, these risks can be neutralised and mitigated. Following this sub-section, the discussion will focus on the Cooja simulator, a useful tool for studying and understanding these attacks in a simulated IoT environment to help develop secure network protocols.

D. COOJA SIMULATOR

The COOJA simulator runs on Contiki OS, a portable operating system with limited resources designed specifically for devices such as sensor nodes [217]. It is built upon an event-driven kernel while also supporting multi-threading. It supports a complete TCP/IP stack through IP and programming protothreads. Simulating sensor nodes based on their real characteristics is the main advantage of the Cooja simulator. The process is carried out by executing program code from ContikiOS and TinyOS using Java Native Interface (JNI). A Java Virtual Machine and C programming (a program-

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

ming language commonly used in firmware sensor nodes) are interconnected by the Java Native Interface. As a result, Cooja can provide accurate simulations of sensor nodes or devices across multiple platforms, including healthcare IoT, closely replicating real-world functionality. Moreover, it is crucial to note that the primary objectives of COOJA are extensibility and plug-in support. In contrast to the interface, the plug-in allows users to interact with the simulator. Plug-ins, for example, enable users to control simulation speeds or observe network traffic between nodes [218]. Cooja also has several inherent tools, including the "radio logger," which records all packets dispatched by nodes in the simulation and associates them with a universal timestamp [30]. As a versatile simulation tool, Cooja allows for research across diverse environments by generating and collecting data for thorough assessments of wireless sensor networks (WSNs) and wireless body area networks (WBANs) in the H-IoT domain. The Cooja simulation can even construct attack scenarios to uncover cybersecurity vulnerabilities within healthcare IoT networks using emulated H-IoT devices.

In order to prevent routing attacks on H-IoT networks, machine learning, and deep learning techniques have been explored. By reviewing examples, it becomes apparent that machine learning and deep learning models perform a significant role in defending against routing attacks in 5G-IoT e-health. Cooja has also been demonstrated as a tool for collecting data from H-IoT devices.

VI. MACHINE LEARNING-DRIVEN INTRUSION AND EVENT DETECTION IN HEALTHCARE-IOT

In order to ensure the security of data within the Healthcare Internet of Things (H-IoT), we need to explore a variety of strategic mechanisms. The section endeavors to illustrate the pivotal role of machine learning in establishing and reinforcing robust security protocols in the Healthcare-IoT, as well as generalized ML techniques and exploring potential cybersecurity applications. Following this, the discussion discusses how feature extraction is essential to identifying threats accurately and mitigating risks. Afterward, a review of intrusion detection systems and event detection systems specifically designed for healthcare environments will be offered, with an emphasis on mechanisms for identifying potential breaches. In order to achieve consistent and reliable threat mitigation, a discourse on the reliability of H-IoT systems is required. The last topic of this section is the potential and challenges associated with convolutional neural networks (CNNs) in the context of IoT security.

A. MACHINE LEARNING TECHNIQUES IN H-IOT CYBERSECURITY

The machine learning method involves the use of data and algorithms to create models that replicate human learning processes. ML algorithms can be refined and optimized by improving an algorithm's loss function [219]. As depicted in Figure 12, ML is traditionally classified into three categories: supervised, unsupervised, and reinforcement learning [220] [221].

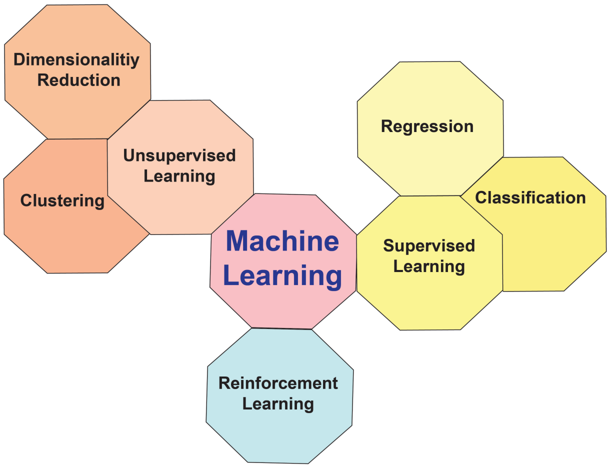

FIGURE 12: **Machine learning techniques for H-IoT cybersecurity**

Over the past several years, machine learning techniques have been successfully applied to a diverse spectrum of cybersecurity challenges [222]. In the specialized domain of healthcare IoT cybersecurity, these techniques have emerged as key assets, significantly enhancing the security level of healthcare devices and systems [223]. As illustrated in Figure 13, several potential use cases are encompassed, including intrusion detection and prevention system, classification of H-IoT devices, anomaly detection and prevention, H-IoT attacks classification, zero-day attack detection, predictive analytics for threat anticipation, identity, and access management (IAM), data breach prediction, Cloud anomaly detection, as well as H-IoT devices behavior analysis. According to Table 2, defenders can identify, evaluate, and mitigate possible threats more precisely with machine learning, as outlined in section IV. Due to this, machine learning algorithms are capable of automating a variety of tasks, including identifying vulnerabilities, deceiving, and disrupting attacks [224]. The following section discusses several potential use cases for ML in H-IoT cybersecurity.

- **Classifying Anomalies in Cybersecurity:** In the classification of threats, machine learning offers a swift and efficient method for processing huge amounts of data. Machine learning analyzes behavior and continuously changes parameters to find anomalies that could indicate attacks [225]. The use of machine learning allows for intelligent security services learning that detects or predicts cyber attacks and anomalies.
- **Predicting and Responding to Data Breaches and Cyber Attacks in Real-time:** With machine learning, large amounts of data can be analyzed from multiple sources to predict cyber threats [226]. A machine learning system is capable of quickly building defensive patches in

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

response to an attack after identifying a cyber threat without human intervention [227].

- **Automating processes:** In the H-IoT cybersecurity sector, machine learning is becoming increasingly crucial, as time-consuming tasks such as vulnerability assessments, malware analysis, network log scrutiny, and intelligence assessments continue to multiply [228]. Automating security workflows enables organizations to respond quickly to threats and incidents, a feat that cannot be achieved through manual efforts alone [229]. Furthermore, automation offers sustainability by enhancing efficiency, and scalability features and reducing unnecessary costs.

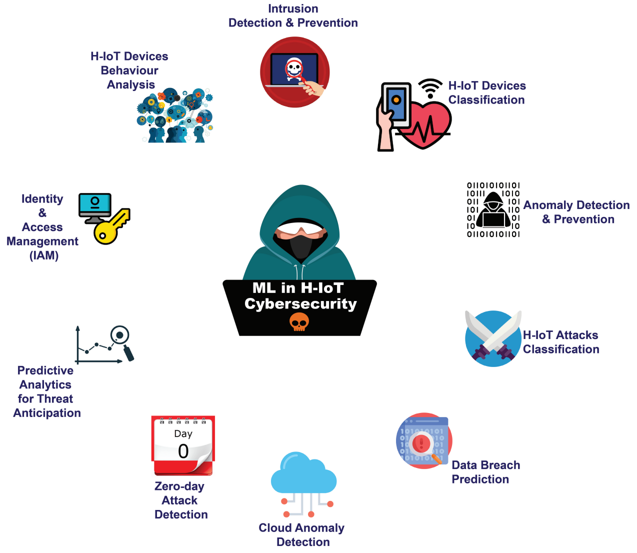
Intrusion Detection & Prevention
H-IoT Devices Behaviour Analysis
H-IoT Devices Classification
Identity & Access Management (IAM)
ML in H-IoT Cybersecurity
Anomaly Detection & Prevention
H-IoT Attacks Classification
Predictive Analytics for Threat Anticipation
Day 0
Zero-day Attack Detection
Data Breach Prediction
Cloud Anomaly Detection

FIGURE 13: **ML use cases for H-IoT cybersecurity**

- **Authentication and Access Control:** Authentication technology is essential for medical devices since it validates a user's credentials with those stored in authorized user systems or authentication servers, enabling access to multiple systems simultaneously [230]. Machine learning determines when to request multi-factor authentication with intelligent authentication.

B. FEATURE EXTRACTION

Healthcare IoT feature extraction is a method for selecting and transforming relevant attributes from data. Moreover, it is necessary to determine the most crucial features before embarking on any ML design process [231]. The use of specific attributes can reduce computing costs and improve storage efficiency [232]. For feature selection, we use the following methods:

- **Filter Methods:** This method calculates the correlation between attributes by comparing the results of their correlations. We select attributes based on statistical methods scores, based on the scores and the threshold values. There are a few methods for extracting features from data that are popular, such as correlation, information gain, and Chi-Square tests [233].
- **Wrapper Methods:** An ML model trains on selected features. The model's accuracy determines whether to include or exclude attributes depending on its reliability within the subset. Eliminating backward and selecting forwards are the most common methods [234].
- **Embedded Methods:** This method combines the benefits of both filters and wrappers (i.e., extracts the best features while maintaining the computational cost). These methods include Least Absolute Shrinkage and Selection Operator (LASSO) regularization, Random Forest [235].

In addition, this stage calculates parameter weights for unique features based on the training set using a DL algorithm. Each DL algorithm has several invisible layers embedded within the inputs and outputs, allowing for the extraction of detailed features [236].

C. INTRUSION DETECTION SYSTEM IN HEALTHCARE-IOT

This section describes healthcare IoT intrusion detection systems in reference to [237]. An intrusion typically targets a network or device's integrity, availability, or confidentiality by impairing its security. Due to the sensitive nature of healthcare data, H-IoT is a lucrative target for attackers, whether external or internal. Monitoring and analyzing device and network activities is automated by IDS solutions, which are available as hardware or software solutions. IDS consists of three components: information source, analysis, and response. Information sources feed data to the analysis component, which, upon identifying an attack, triggers a response - either passively such as notifications, or actively such as disabling communication.

In [238], the authors propose a 5G-driven healthcare landscape, where remote patient monitoring is enabled by the Internet of Medical Things (IoMT). Nevertheless, ensuring the security of data remains a challenge. A new lightweight Intrusion Detection System (IDS) for IoMT, utilizing kernel techniques for feature selection, and a kernel extreme learning machine for decision-making, is introduced. This IDS detected anomalies with 99.9% accuracy on the dataset WUSTL-EHMS-2020.

In [239], the authors used mobile agents to detect intrusions in a medical environment. Furthermore, a simulation of hospital network topology was conducted to conduct IoMT experiments, which included the identification of network-level intrusions using machine learning and regression algorithms, and the implementation of various digital imaging and communications in medicine (DICOM) protocols by connected devices such as ultrasound scanners and MRI machines, utilizing wireless body area networks (WBAN). Wireless body area networks are composed of wearable and implantable devices that transmit physiological data continuously, allowing patients to be monitored, diagnosed, and treated continuously. In total, 72 independent simulations were conducted across

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

216 network types, resulting in an overall best- and worst-case detection accuracy of 99.9% and 92.91%, respectively.

In [240], the proposed system integrates ensemble learning and cloud-based architecture to detect cyberattacks. In this ensemble setup, Decision Trees, Naive Bayes, and Random Forests are used as individual learners at the initial level. In the following level, XGBoost uses the classification results to differentiate between normal and attack cases. Using large-scale, diverse IoT networks, ToN-IoT provides an accurate dataset for the model. Experimental results indicate that the proposed framework can achieve a detection rate of 99.98%, a precision of 96.98%, and a reduction in false alarms.

By demonstrating significant accuracy and reduced false alarms in cybersecurity, these examples show that machine learning enhances intrusion detection systems in H-IoT.

D. EVENT DETECTION SYSTEM

A healthcare IoT system uses event detection to identify and capture significant occurrences and incidents. An event detection algorithm analyzes sensor data, network traffic, and device interactions to detect patterns, anomalies, and predefined triggers that indicate critical events, such as emergencies, device malfunctions, and abnormal patient conditions. Several machine learning techniques investigate classification, including supervised, unsupervised, and reinforcement learning. A supervised learning algorithm employs a labeled dataset for training that is used to determine the relationship between inputs and outputs. Based on the correlation between the input samples, unsupervised learning algorithms can classify the provided data into clusters. The third category of algorithms is reinforcement learning and online learning. These algorithms utilize current knowledge and explore the environment to classify the data [241] [242].

E. RELIABILITY IN HEALTHCARE-IOT SYSTEMS

Data exchange between e-health systems must be reliable and efficient in H-IoT for enabling cyber resilience, security metrics (Confidentiality, Integrity, Availability (CIA) Triad), and controls within the ecosystem [1] [134] [243]:

- **Confidentiality:** It is illegal for unauthorized individuals to access medical information.
- **Integrity:** There is no possibility of adversaries altering data during transit or storage.
- **Non-repudiation:** Data transmission and reception are inevitable.
- **Data Freshness:** There is no way to re-generate old data.
- **Resilience to Attacks:** The system should adapt to failed nodes, and there should be no single point of failure.
- **Data Authentication:** It is necessary to authenticate the addresses and object information retrieved.
- **Access Control:** Providing access control to data is a requirement for information providers.
- **Client Privacy:** A lookup system should only be able to infer its purpose from the information provider.
- **Fault Tolerance and Self-healing:** An IoT device or battery energy failure should not disrupt health service continuity.

F. CONVOLUTIONAL NEURAL NETWORK (CNN) IN HEALTHCARE-IOT

Using Convolutional Neural Networks (CNNs) has been demonstrated to be significantly more effective than previous methods in identifying threats, surpassing techniques like Decision Trees, SVM, and K-nearest neighbor (KNN) [244]. In classification problems, CNNs are used as feed-forward networks [245]. Essentially, CNNs are characterized by two processes. First, convolution involves transforming inputs into outputs using a series of filters or kernels. In particular, CNNs have streamlined image recognition to the point where it is self-contained, obviating the need for external image processing software. Furthermore, CNNs are capable of recognizing outcomes efficiently and adapting seamlessly to changing identification criteria. Moreover, their ability to leverage preexisting networks enhances system versatility and applicability [246]. Neurons are arranged in layers in a three-dimensional configuration, spanning width, height, and depth. This is illustrated in 14, which illustrates a CNN architecture for analyzing H-IoT data.

As part of the architecture of Convolutional Neural Networks (CNNs), the initial layer, called Layer 1, is composed of a significant number of neurons to effectively process input data [247]. convolutional neural networks (CNNs) have three fundamental parameters: dataset size, quality, and type. Multiple receptive layers can be used to effectively process input layers. In this configuration, overlapping input regions are created, allowing high-resolution outputs from the original input. For detecting features, CNNs employ operations such as pooling and convolution. Using the fully connected layer as a classifier follows the process of extracting features. Typically, CNN architecture, convolutional, and pooling layers are merged, though it is not mandatory.

Rectified Linear Unit (ReLU): In neural networks, ReLUs follow convolution modules. The primary function of ReLU is to activate specific neurons within the network. The Rectified Linear Unit (ReLU) keeps the values of active neurons while converting inactive neurons to *0* using a simple threshold [248] [249]. The activation information retained by this segment of the neural network remains significant for future inferences made by other segments of the network.

An activation function such as the ReLU is essential for introducing nonlinear operations into inherently linear neural networks. Adding nonlinearity to the network increases its ability to fit data accurately, so it can capture intricate patterns and relationships.

The ReLU activation function does not alter the dimensions of the input or output data. A mathematical expression for this function can be found in equation 1 (1)

$$y = \max\{0, x\} \tag{1}$$

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

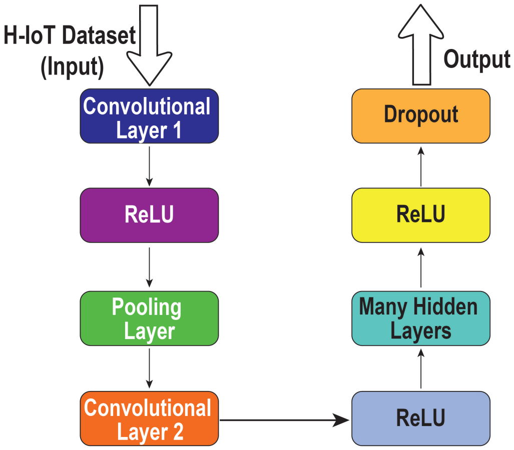

FIGURE 14: **The Convolutional Neural Network architecture**

Pooling Layer: Pooling layers contribute significantly to CNN performance by strategically inserting them between CNN layers. By reducing the number of network parameters and downsampling the data, this integration achieves two objectives: increasing computational efficiency and reducing computation time. Furthermore, the downsampling process, which is more precise than average pooling, preserves texture information by minimizing discrepancies in evaluation values resulting from the convolutional layers [250] [251]. Max pooling stands out as an essential technique because it is capable of detecting and retaining the maximum value within each receptive field. Consequently, it preserves essential features while reducing data dimensions and in each window, it displays the maximum value [252].

Fully Connected Layer: The Fully Connected Layer follows the pooling and convolution layers. Based on the features extracted by the previous layers, this layer classifies the input data. The activation functions of the neurons in this layer perform a significant role in processing the information from the preceding layer. Fully connected neurons allow the network to recognize complex patterns and relations. According to [214], CNN deep learning classifiers can be used to identify malware instances in healthcare datasets. This research demonstrates the network's capability to analyze intricate data and provide valuable insight into a number of domains that are vital to human health and security.

Softmax: The Softmax activation functions are commonly assigned to the neural networks' final layer to perform multi-class classification. Data can be transformed using the Softmax function into a probability distribution from *0* to *1* with a sum of *1*. As a result of the function, the classification of data is easier since it emphasizes differences between input values. According to Sharma et al. [253], a CNN-Bidirectional LSTM architecture is proposed for using deep learning in smart healthcare networks for intrusion detection. Using softmax activation functions, the model detects DDoS attacks by classifying traffic flows as benign or malicious. Faruqui et al. [254] propose SafetyMed, a specialized Intrusion Detection System (IDS) for securing the Internet of Medical Things (IoMT). IoMT-specific intrusions are identified with SafetyMed using CNN and LSTM. In the output layer, Softmax activation functions are used to convert raw scores into probabilities ranging from 0 to 1. This enhances the accuracy of the decision-making process. IoMT vulnerabilities are effectively addressed by SafetyMed, which has an average detection accuracy of 97.63%.

The scope of this section encompassed a wide range of machine learning techniques, applications, and advanced CNN-based mechanisms illuminating multifaceted strategies for the protection of healthcare IoT devices.

VII. SECURITY AND PRIVACY IN H-IOT ENVIRONMENTS

This section emphasizes the importance of effective safeguards and rigorous protocols to protect sensitive data and preserve user confidentiality in H-IoT environments. In-depth analysis explores key challenges, effective strategies, and emerging trends. IoT is being transformed into a network of interconnected devices, where security and privacy are becoming crucial challenges. Therefore, the IoT network is built around anomaly detection techniques. In the IoT, anomaly detection algorithms detect abnormal behaviors instantly, preventing serious problems from occurring. However, healthcare and the IoT combine to raise the stakes even higher. As a result, machine learning could potentially provide remedies for these challenges. Additionally, a machine learning-based architecture for anomaly detection is described in detail in the section.

A. ANOMALY DETECTION

The term anomaly refers to data segments that do not follow the expected pattern or features of the rest of the data. Anomaly detection is crucial since anomalous activities contain critical information and relevance [255]. Anomaly detection involves several independent processes in H-IoT, as illustrated in Figure 15. Data collection is the first step in this architecture. Following the creation of the dataset, it should be analyzed thoroughly to determine the data types.

Besides, the data is preprocessed before being analyzed. The preprocessing of data includes filtering, visualizing, and extracting features. These steps convert the data into feature vectors. It is then necessary to divide the feature vectors into training and testing sets to an 80:20 ratio. The Learning Algorithm develops an optimal final model by utilizing the training set. It is possible to use a variety of classifiers to experiment with the most accurate accuracy [256].

With 5G networks facilitating rapid, voluminous data exchanges, the Internet of Medical Things (IoMT) has gained momentum in the healthcare sector. In [257], the emphasis is on detecting anomalies using deep learning for enhanced security within 5G contexts in IoM. By utilizing multi-model autoencoders for feature extraction, the complexity of traffic

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

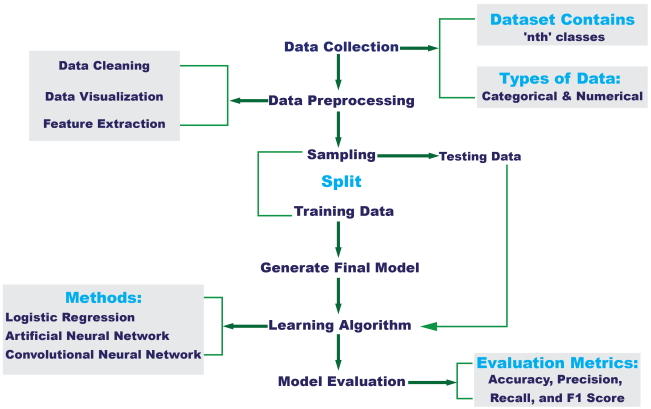
Data Collection
Dataset Contains 'nth' classes
Types of Data: Categorical & Numerical
Data Cleaning
Data Visualization
Feature Extraction
Data Preprocessing
Sampling
Testing Data
Split
Training Data
Generate Final Model
Methods:
Logistic Regression
Artificial Neural Network
Convolutional Neural Network
Learning Algorithm
Model Evaluation
Evaluation Metrics:
Accuracy, Precision, Recall, and F1 Score

FIGURE 15: **ML-based anomaly detection architecture in H-IoT**

feature information has been significantly reduced. A new algorithm for the detection of multi-featured sequence anomalies is also presented, which is optimized to cope with the high data volume of 5G networks. It has been demonstrated that deep learning combined with 5G technology can identify and mitigate anomalies efficiently, thereby increasing IoMT systems' resilience and reliability.

B. BEST PRACTICES FOR ENABLING DATA PRIVACY, SECURITY AND BUILDING RISK MITIGATION STRATEGIES IN SMART ENVIRONMENTS

Digital healthcare environments [258] are becoming more prevalent despite numerous security and privacy concerns and they are susceptible to a unique set of challenges (i.e., securing the massive amount of healthcare data harvested every second from thousands of connected IoT devices). Healthcare procedures and decisions are made based on this data, in situations where this data is compromised, breached this may result in a wrong diagnosis/treatment affecting the human life. Securing smart environments requires implementing defense-in-depth strategies and multiple layers of security across the ecosystem such as: (i) Standards and data governance risk and control (DGRC) policies for access control, data protection, encryption, remote access (ii) Monitoring and response mechanisms for Security Information and Event Management (SIEM), identity and access management, log analysis, cyber forensics, (iii) Perimeter controls for intrusion detection, prevention and next generation firewalls, (iv) Securing the network using VPN services, web-filtering, securing remote services and site-to-site connections (v) Hardening end-point security by enabling Zero Trust mechanisms, patching the systems with latest updates to mitigate vulnerabilities, using an up-to-date antivirus tool to detect and protect the end-point for new vulnerabilities, (vi) the human element is the weakest link and its essential to build cyber awareness within the workplace environment and train them so that they are cyber prepared, (vii) enabling application security using vulnerability scanners and making sure that only inventoried tools are used, (viii) last but not the least, to ensure data security mechanisms are in place (i.e. end-to-end secured data, data classification and have a data loss prevention/backup strategy) [1]. However, as mentioned earlier due to generative AI the impact and frequency of cyber attacks has escalated. Since the attacks are constantly evolving and new threats are coming to surface, there is a possibility that the novel threats would go undetected. This is why there is an essential need for a versatile Machine Learning solution to neutralise and mitigate these threats.

C. MITIGATING HEALTHCARE-IOT SECURITY AND PRIVACY THREATS USING MACHINE LEARNING

The security and privacy of sensitive health information has become a worldwide concern. In healthcare security and privacy, machine learning-based solutions are essential among cryptographic, password-based, and digital signature-based solutions. As shown in Figure 16, machine learning models can detect Device Spoofing and Identity Impersonation, Intrusion Detection and Prevention, and Device Authentication. An ML model can prevent anomalies after detection. As a result, ML models perform a significant role in H-IoT [259]. In healthcare systems, Hau et al. applied machine learning techniques to increase security and privacy [260]. Begli et al. implemented SVM-based intrusion detection to monitor remote healthcare [261]. Sengan et al. developed an adaptive, ML-driven routing system for healthcare data security [262].

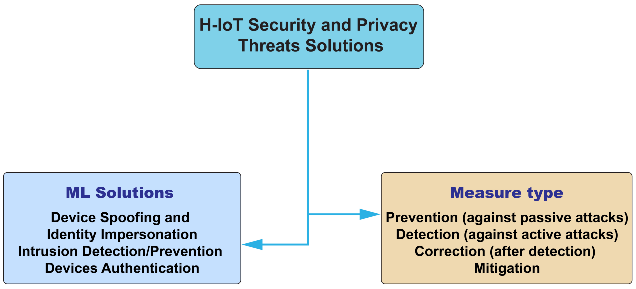
H-IoT Security and Privacy Threats Solutions
ML Solutions
Device Spoofing and Identity Impersonation
Intrusion Detection/Prevention
Devices Authentication
Measure type
Prevention (against passive attacks)
Detection (against active attacks)
Correction (after detection)
Mitigation

FIGURE 16: **H-IoT security and privacy threat solution**

VIII. IMPACT OF HEALTHCARE-IOT TECHNOLOGIES IN THE FUTURE

Healthcare and smart cities benefit greatly from the Internet of Things (IoT). This technology will significantly change everyday life and cityscapes in the coming years. This section discusses the potential impact of healthcare IoT on smart cities, including relevant challenges and innovative solutions. Quality of service is integral to this discussion, which entails ensuring the reliability of services. Furthermore, H-IoT networks can be made more flexible, scalable, resource-efficient, and secure with the help of Software-Defined Networks (SDNs).

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

A. FUTURE OF HEALTHCARE-IOT TECHNOLOGIES

People expect H-IoT systems to integrate with their living environments. The future of infrastructure lies in smart cities. As a result, affiliating the H-IoT system within modern city architecture facilitates widespread deployment of the H-IoT [263]. A significant role in smart cities, Software-defined networking (SDN) plays a significant role in H-IoT systems. Using SDN in H-IoT, cities can gain more efficient management, more secure provision of services, effective resource allocation, and overall better performance.

B. CHALLENGES

Despite the growing popularity of IoT applications in healthcare, several challenges hinder their implementation. In the following section, we explore key challenges connected to H-IoT development [264].

Heterogeneous Networks: Developing H-IoT requires devices to coexist and inter-operate across diverse networks and operating systems. Among the technologies used in communication are Bluetooth, IrDA, UWB, Zigbee, WLANs, Wi-Fi 6, and 5G. Batteries drain out faster when communicating over long distances [265]. It is essential that these devices, regardless of their heterogeneity in implementation and communication, can identify and communicate with each other.

Quality of Service (QoS): Healthcare IoT is characterized by low latency and low power consumption. There is a risk to a patient's health when dealing with issues related to the Internet of Things. Consequently, H-IoT signals should be transmitted and processed with the least possible delay. High-bandwidth networking resources can be used to achieve this [266]. A 5G network, with its ability to ensure quality of service through rapid data transmission, minimal latency, and extensive connectivity, presents itself as an ideal solution for healthcare IoT applications [267]. In this context, quality of service refers to a system's ability to provide a minimum level of performance and reliability and to ensure accurate and timely transmission and reception of data.

Privacy and Security: In H-IoT, the privacy and security of patients and their data are paramount as any compromise could result in severe consequences (i.e., loss of command and control of a cobot arm used for precision surgeries may lead to its malfunctioning causing harms to person, property, loss of availability could lead to healthcare service disruption leaving critical patients who may need immediate attention vulnerable, loss of integrity would risk patients to wrong diagnosis or medication, loss of confidentiality would lead to loss of privacy, digital identity frauds, deep fakes, biohacking issues, etc.). In many cases, H-IoT uses heterogeneous networks to communicate and store data, exposing it to attack over long distances [268]. Thus, the security and privacy of data require anomaly detection, mitigation, robust encryption, and authentication techniques as mentioned in section VII-B. However, in designing and implementing the defense-in-depth techniques, it is necessary to consider the resource constraints of the devices involved in H-IoT, and the developed solutions should be lightweight and energy-efficient.

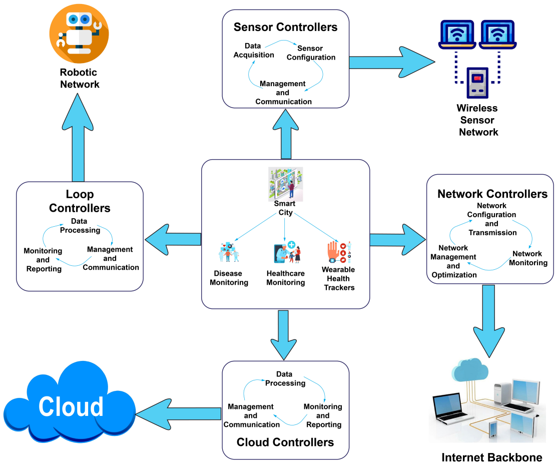

FIGURE 17: **Software defined network-based H-IoT**

C. SOFTWARE-DEFINED NETWORK (SDN) IN HEALTHCARE-IOT

An emerging paradigm in computer networking is software-defined networking (SDN). Data planes, control planes, and application planes are the three tiers of SDN. Data and control planes are separated to improve network performance. In contrast, traditional architectures combine both data and control planes onto one device, while SDN separates them to simplify network management [269], [270]. SDNs forward packets according to predefined policies [271]. SDN-based H-IoT consists of Sensor Controllers, Cloud Controllers, Network Controllers, and Closed-Loop Controllers, which provide four types of services: data acquisition, network configuration and transmission, processing, and actionable feedback, as illustrated in Figure 17.

The software-defined network is used by Google, for example, to manage its wide-area network traffic [272]. The network infrastructure increasingly relies on SDNs, and protecting a network from attack is crucial to ensure its integrity and availability [273]. In [274], a novel software-defined network (SDN) architecture is presented, incorporating a new controller and load-balancing algorithms based on machine learning for the Internet of Medical Things (IoMT). A support vector machine algorithm, which achieved 95.1% accuracy through extensive simulations, validates the architecture's effectiveness. In preparation for broader 5G integration, this approach represents an important advance in healthcare IoT. Adding deep learning to SDNs makes healthcare IoT services, such as telemedicine, more reliable and secure [275]. Using a software-defined network system, [276] illustrates the process of communicating between medical services and nano-networks inside people's bodies. A certain set of software rules controls this method, which makes healthcare more efficient.

IX. CONCLUSION

This paper deep dives into the fundamental elements and practical applications of the digital Healthcare Internet of Things (H-IoT). It discusses the essential technologies and methodologies for optimizing these systems within Healthcare 5.0. The research focuses on various cyber threats, vulnerabilities, and cyber attacks carried out at the different IoT layers and explores the security and privacy of healthcare IoT through deep neural networks and artificial intelligence. A demonstration of a cloud-based solution and big data analytics using IoT and software-defined networks is provided that illustrates the advantages associated with a precise, efficient, and secured healthcare ecosystem. The authors also provide insights on the security challenges related to wireless and communication technologies (i.e., 5G) in H-IoT and how the ML algorithms can enable the digital healthcare environment to bridge those security gaps.

ACKNOWLEDGMENT

This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number 18/CRT/6049.

REFERENCES

[1] L. L. Dhirani, E. Armstrong, and T. Newe, “Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap,” *Sensors*, vol. 21, no. 11, p. 3901, 2021.

[2] S. Zardari, N. Nisar, Z. Fatima, and L. L. Dhirani, “Iot–assets taxonomy, threats assessment and potential solutions,” in *2023 Global Conference on Wireless and Optical Technologies (GCWOT)*. IEEE, 2023, pp. 1–8.

[3] S. Latif, J. Qadir, S. Farooq, and M. A. Imran, “How 5g (and concomitant technologies) will revolutionize healthcare,” *arXiv preprint arXiv:1708.08746*, 2017.

[4] S. Majumder, T. Mondal, and M. J. Deen, “Wearable sensors for remote health monitoring,” *Sensors*, vol. 17, no. 1, p. 130, 2017.

[5] N. Wickramasinghe and F. Bodendorf, *Delivering superior health and wellness management with IoT and analytics*. Springer, 2019.

[6] O. Postolache, D. J. Hemanth, R. Alexandre, D. Gupta, O. Geman, and A. Khanna, “Remote monitoring of physical rehabilitation of stroke patients using iot and virtual reality,” *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 562–573, 2020.

[7] P. K. Gupta, M. H. Nawaz, S. S. Mishra, K. Parappa, A. Silla, and R. Hanumegowda, “New age approaches to predictive healthcare using in silico drug design and internet of things (iot),” *Sustainable and Energy Efficient Computing Paradigms for Society*, pp. 127–151, 2021.

[8] M. Jayashankara, S. S. Udmale, A. K. Pandey, and R. S. Singh, “Iot healthcare architecture,” in *IoT-Based Data Analytics for the Healthcare Industry*. Elsevier, 2021, pp. 9–29.

[9] C. A. Tavera, J. H. Ortiz, O. I. Khalaf, D. F. Saavedra, T. H. Aldhyani *et al.*, “Wearable wireless body area networks for medical applications,” *Computational and Mathematical Methods in Medicine*, vol. 2021, 2021.

[10] D. Gangwani, “Ai-and iot-based body sensor networks for healthcare system,” *Artificial Intelligence in Cyber-Physical Systems: Principles and Applications*, vol. 2, p. 17, 2023.

[11] . D. Inc, “Edge to core and the internet of things and data placement,” *infohub*, 2023. [Online]. Available: https://tinyurl.com/mwj4ywfb

[12] A. P. Plageras and K. E. Psannis, “Algorithms for big data delivery over the internet of things,” in *2017 IEEE 19th Conference on Business Informatics (CBI)*, vol. 1. IEEE, 2017, pp. 202–206.

[13] M. Usak, M. Kubiatko, M. S. Shabbir, O. Viktorovna Dudnik, K. Jermsittiparsert, and L. Rajabion, “Health care service delivery based on the internet of things: A systematic and comprehensive study,” *International Journal of Communication Systems*, vol. 33, no. 2, p. e4179, 2020.

[14] S. M. Karunarathne, N. Saxena, and M. K. Khan, “Security and privacy in iot smart healthcare,” *IEEE Internet Computing*, vol. 25, no. 4, pp. 37–48, 2021.

[15] A. Hanson and L. Haddad, “Nursing rights of medication administration. statpearls,” *Treasure Island (FL): StatPearls Publishing*, 2022.

[16] M. Ciampi, A. Coronato, M. Naeem, and S. Silvestri, “An intelligent environment for preventing medication errors in home treatment,” *Expert Systems with Applications*, vol. 193, p. 116434, 2022.

[17] G. Muhammad, M. S. Hossain, and N. Kumar, “Eeg-based pathology detection for home health monitoring,” *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 603–610, 2020.

[18] L. Shrotriya, K. Sharma, D. Parashar, K. Mishra, S. S. Rawat, and H. Pagare, “Apache spark in healthcare: Advancing data-driven innovations and better patient care,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, 2023.

[19] S. U. Amin and M. S. Hossain, “Edge intelligence and internet of things in healthcare: A survey,” *IEEE Access*, vol. 9, pp. 45–59, 2020.

[20] T. Shaik, X. Tao, N. Higgins, L. Li, R. Gururajan, X. Zhou, and U. R. Acharya, “Remote patient monitoring using artificial intelligence: Current state, applications, and challenges,” *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 13, no. 2, p. e1485, 2023.

[21] K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar, and A. Khan, “An intelligent iot based healthcare system using fuzzy neural networks,” *Scientific programming*, vol. 2020, pp. 1–15, 2020.

[22] A. A. Al-Atawi, F. Khan, and C. G. Kim, “Application and challenges of iot healthcare system in covid-19,” *Sensors*, vol. 22, no. 19, p. 7304, 2022.

[23] J. Mao, P. Zhou, X. Wang, H. Yao, L. Liang, Y. Zhao, J. Zhang, D. Ban, and H. Zheng, “A health monitoring system based on flexible triboelectric sensors for intelligence medical internet of things and its applications in virtual reality,” *arXiv preprint arXiv:2309.07185*, 2023.

[24] V. Subramaniyaswamy, G. Manogaran, R. Logesh, V. Vijayakumar, N. Chilamkurti, D. Malathi, and N. Senthilselvan, “An ontology-driven personalized food recommendation in iot-based healthcare system,” *The Journal of Supercomputing*, vol. 75, pp. 3184–3216, 2019.

[25] P. He, C. Lan, Y. Cui, R. Wang, and D. Wu, “Accelerated federated learning with dynamic model partitioning for h-iot,” in *2023 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2023, pp. 1–6.

[26] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, “Privacy enhancing technologies in the internet of things: Perspectives and challenges,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2159–2187, 2018.

[27] F. Subhan, A. Mirza, M. B. M. Su’ud, M. M. Alam, S. Nisar, U. Habib, and M. Z. Iqbal, “Ai-enabled wearable medical internet of things in healthcare system: A survey,” *Applied Sciences*, vol. 13, no. 3, p. 1394, 2023.

[28] S. Swain, B. Bhushan, G. Dhiman, and W. Viriyasitavat, “Appositeness of optimized and reliable machine learning for healthcare: a survey,” *Archives of Computational Methods in Engineering*, vol. 29, no. 6, pp. 3981–4003, 2022.

[29] S. S. Gopalan, A. Raza, and W. Almobaideen, “Iot security in healthcare using ai: A survey,” in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*. IEEE, 2021, pp. 1–6.

[30] N. Finne, J. Eriksson, T. Voigt, G. Suciu, M.-A. Sachian, J. Ko, and H. Keipour, “Multi-trace: multi-level data trace generation with the cooja simulator,” in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2021, pp. 390–395.

[31] H. K. Bharadwaj, A. Agarwal, V. Chamola, N. R. Lakkaniga, V. Hassija, M. Guizani, and B. Sikdar, “A review on the role of machine learning in enabling iot based healthcare applications,” *IEEE Access*, vol. 9, pp. 38 859–38 890, 2021.

[32] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, “A systematic review of iot in healthcare: Applications, techniques, and trends,” *Journal of Network and Computer Applications*, vol. 192, p. 103164, 2021.

[33] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, “The future of healthcare internet of things: a survey of emerging technologies,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[34] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, “Secure and robust machine learning for healthcare: A survey,” *IEEE Reviews in Biomedical Engineering*, vol. 14, pp. 156–180, 2020.

[35] G. Karthick and P. Pankajavalli, “A review on human healthcare internet of things: a technical perspective,” *SN Computer Science*, vol. 1, no. 4, p. 198, 2020.

[36] F. T. Al-Dhief, N. M. A. Latiff, N. N. N. A. Malik, N. S. Salim, M. M. Baki, M. A. A. Albadr, and M. A. Mohammed, “A survey of voice

pathology surveillance systems based on internet of things and machine learning algorithms," *IEEE Access*, vol. 8, pp. 64 514–64 533, 2020.

[37] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of internet of things in healthcare: a systematic literature review and classification," *Universal Access in the Information Society*, vol. 18, pp. 837–869, 2019.

[38] K. Shailaja, B. Seetharamulu, and M. Jabbar, "Machine learning in healthcare: A review," in *2018 Second international conference on electronics, communication and aerospace technology (ICECA)*. IEEE, 2018, pp. 910–914.

[39] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (iomt)," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019, pp. 457–464.

[40] S. K. Jagatheesaperumal, P. Mishra, N. Moustafa, and R. Chauhan, "A holistic survey on the use of emerging technologies to provision secure healthcare solutions," *Computers and Electrical Engineering*, vol. 99, p. 107691, 2022.

[41] M. M. Dhanvijay and S. C. Patil, "Internet of things: A survey of enabling technologies in healthcare and its applications," *Computer Networks*, vol. 153, pp. 113–131, 2019.

[42] S. Ketu and P. K. Mishra, "Internet of healthcare things: A contemporary survey," *Journal of Network and Computer Applications*, vol. 192, p. 103179, 2021.

[43] S. K and N. D. C, "Advancements and challenges in 5g networks," in *2023 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES)*, 2023, pp. 1–6.

[44] K. Bawaneh, F. Ghazi Nezami, M. Rasheduzzaman, and B. Deken, "Energy consumption analysis and characterization of healthcare facilities in the united states," *Energies*, vol. 12, no. 19, p. 3775, 2019.

[45] E. Kost. (2023) 14 biggest healthcare data breaches [updated 2023]. [Online]. Available: https://tinyurl.com/axrpc6x5

[46] T. E. U. A. for Cybersecurity (ENISA). (2023) Enisa foresight cybersecurity threats for 2030. [Online]. Available: https://tinyurl.com/3ahnvds7

[47] N. Chaurasia and P. Kumar, "A comprehensive study on issues and challenges related to privacy and security in iot," *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, p. 100158, 2023.

[48] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the internet of things." *Int. J. Comput. Intell. Syst.*, vol. 12, no. 1, pp. 39–58, 2018.

[49] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the internet of things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64–71, 2016.

[50] H. R. Abdulqadir, S. R. Zeebaree, H. M. Shukur, M. M. Sadeeq, B. W. Salim, A. A. Salih, and S. F. Kak, "A study of moving from cloud computing to fog computing," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 60–70, 2021.

[51] A. R. Chordiya, S. Majumder, and A. Y. Javaid, "Man-in-the-middle (mitm) attack based hijacking of http traffic using open source tools," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*. IEEE, 2018, pp. 0438–0443.

[52] J. M. Alkhathami and S. M. Alzahrani, "Detection of sql injection attacks using machine learning in cloud computing platform," *Journal Of Theoretical And Applied Information Technology*, vol. 100, no. 15, 2022.

[53] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking—a review," in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*. IEEE, 2017, pp. 1–6.

[54] A. Malik, B. Bhushan, S. Bhatia Khan, R. Kashyap, R. Chaganti, and N. Rakesh, "Security attacks and vulnerability analysis in mobile wireless networking," in *5G and Beyond*. Springer, 2023, pp. 81–110.

[55] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th international conference for internet technology and secured transactions (ICITST)*. IEEE, 2015, pp. 336–341.

[56] N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Yusupov, and D. Kodirov, "Architecture, protocols, and applications of the internet of medical things (iomt)," *J. Commun*, vol. 17, no. 11, pp. 900–918, 2022.

[57] A. M. Albalawi and M. A. Almaiah, "Assessing and reviewing of cybersecurity threats, attacks, mitigation techniques in iot environment," *J. Theor. Appl. Inf. Technol*, vol. 100, pp. 2988–3011, 2022.

[58] A. Bekkali, M. Essaaidi, M. Boulmalf, and D. Majdoubi, "Systematic literature review of internet of things (iot) security," *Adv. Indynamical Syst. Appl.(ADSA)*, vol. 21, pp. 25–39, 2022.

[59] S. Zaman, M. R. Khandaker, R. T. Khan, F. Tariq, and K.-K. Wong, "Thinking out of the blocks: Holochain for distributed security in iot healthcare," *IEEE Access*, vol. 10, pp. 37 064–37 081, 2022.

[60] V. Mohindru and A. Garg, "Security attacks in internet of things: A review," *Recent Innovations in Computing: Proceedings of ICRIC 2020*, pp. 679–693, 2021.

[61] R. Khader and D. Eleyan, "Survey of dos/ddos attacks in iot," *Sustainable Engineering and Innovation*, vol. 3, no. 1, pp. 23–28, 2021.

[62] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, 2017.

[63] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data collection and wireless communication in internet of things (iot) using economic analysis and pricing models: A survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2546–2590, 2016.

[64] I. Cvitić, M. Vujić *et al.*, "Classification of security risks in the iot environment." *Annals of DAAAM & Proceedings*, vol. 26, no. 1, 2015.

[65] J. DiMaggio, *The Art of Cyberwarfare: An Investigator's Guide to Espionage, Ransomware, and Organized Cybercrime*. No Starch Press, 2022.

[66] A. Roohi, M. Adeel, and M. A. Shah, "Ddos in iot: a roadmap towards security & countermeasures," in *2019 25th International Conference on Automation and Computing (ICAC)*. IEEE, 2019, pp. 1–6.

[67] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice," *Journal of Hardware and Systems Security*, vol. 2, pp. 97–110, 2018.

[68] M. Adil, R. Khan, J. Ali, B.-H. Roh, Q. T. H. Ta, and M. A. Almaiah, "An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment," *IEEE Access*, vol. 8, pp. 163 209–163 224, 2020.

[69] M. N. Khan, H. U. Rahman, M. A. Almaiah, M. Z. Khan, A. Khan, M. Raza, M. Al-Zahrani, O. Almomani, and R. Khan, "Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks," *IEEE Access*, vol. 8, pp. 176 495–176 520, 2020.

[70] M. H. Qasem, N. Obeid, A. Hudaib, M. A. Almaiah, A. Al-Zahrani, and A. Al-Khasawneh, "Multi-agent system combined with distributed data mining for mutual collaboration classification," *IEEE Access*, vol. 9, pp. 70 531–70 547, 2021.

[71] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6461–6471, 2020.

[72] A. K. Al Hwaitat, M. A. Almaiah, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, "Improved security particle swarm optimization (pso) algorithm to detect radio jamming attacks in mobile networks," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, 2020.

[73] M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha, and M. A. Alohali, "A lightweight hybrid deep learning privacy preserving model for fc-based industrial internet of medical things," *Sensors*, vol. 22, no. 6, p. 2112, 2022.

[74] M. A. Almaiah, F. Hajjej, A. Ali, M. F. Pasha, and O. Almomani, "A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare iot based cps," *Sensors*, vol. 22, no. 4, p. 1448, 2022.

[75] F. Almudaires and M. Almaiah, "Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation," in *2021 International Conference on Information Technology (ICIT)*. IEEE, 2021, pp. 732–738.

[76] Y. Alotaibi and M. Ilyas, "Security risks in internet of things (iot): a brief survey," in *Proceedings of the 26th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2022)*, 2022, pp. 1–5.

[77] Y. Chahid, M. Benabdellah, and A. Azizi, "Internet of things protocols comparison, architecture, vulnerabilities and security: State of the art," in *Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems*, 2017, pp. 1–6.

[78] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "Cybersecurity: a review of internet of things (iot) security issues, challenges and techniques," in *2019 2nd International Conference on Com-*

puter Applications & Information Security (ICCAIS). IEEE, 2019, pp. 1–6.

[79] H. N. Security, "As biohacking evolves, how vulnerable are we to cyber threats?" *Help Net Security*, 2023. [Online]. Available: https://tinyurl.com/yts6bmr3

[80] V. Varadharajan, U. Tupakula, and K. Karmakar, "Study of security attacks against iot infrastructures," Technical Report TR1: ISIF ASIA Funded Project, Tech. Rep., 2018.

[81] S. E. digital future, "Cyber resilience act," *digital-strategy*, 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[82] S. Sinha *et al.*, "Impact of dos attack in iot system and identifying the attacker location for interference attacks," in *2021 6th international conference on communication and electronics systems (ICCES)*. IEEE, 2021, pp. 657–662.

[83] S. E. digital future, "Directive on measures for a high common level of cybersecurity across the union (nis2 directive)," *digital-strategy*, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[84] P. AG. (2023) Complete guide to gdpr compliance. [Online]. Available: https://gdpr.eu/

[85] M. M. Nasralla, I. García-Magariño, and J. Lloret, "Defenses against perception-layer attacks on iot smart furniture for impaired people," *IEEE Access*, vol. 8, pp. 119 795–119 805, 2020.

[86] M. Sugadev, S. J. Rayen, J. Harirajkumar, R. Rathi, G. Anitha, S. Ramesh, and K. Ramaswamy, "Implementation of combined machine learning with the big data model in iomt systems for the prediction of network resource consumption and improving the data delivery," *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[87] I. Alihamidi, A. A. Madi, and A. Addaim, "Proposed architecture of e-health iot," in *2019 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 2019, pp. 1–7.

[88] H. I. Ahmed, A. A. Nasr, S. Abdel-Mageid, and H. K. Aslan, "A survey of iot security threats and defenses," *International Journal of Advanced Computer Research*, vol. 9, no. 45, pp. 325–350, 2019.

[89] E. A. Hagras, S. Aldosary, H. Khaled, and T. M. Hassan, "Physical layer authenticated image encryption for iot network based on biometric chaotic signature for mpfrft ofdm system," *Sensors*, vol. 23, no. 18, p. 7843, 2023.

[90] Y. Zhu and M. Xu, "Enhancing network throughput via the equal interval frame aggregation scheme for ieee 802.11 ax wlans," *Chinese Journal of Electronics*, vol. 32, no. 4, pp. 747–759, 2023.

[91] M. Chotalia and S. Gajjar, "Performance comparison of ieee 802.11 ax, 802.11 ac and 802.11 n using network simulator ns3," in *International Conference on Computing Science, Communication and Security*. Springer, 2023, pp. 191–203.

[92] S. S. Sefati and S. Halunga, "Ultra-reliability and low-latency communications on the internet of things based on 5g network: Literature review, classification, and future research view," *Transactions on Emerging Telecommunications Technologies*, p. e4770, 2023.

[93] A. Anjum, P. Agbaje, A. Mitra, E. Oseghale, E. Nwafor, and H. Olufowobi, "Towards named data networking technology: Emerging applications, use cases, and challenges for secure data communication," *Future Generation Computer Systems*, 2023.

[94] D. C. Valadares, N. C. Will, Á. Á. C. Sobrinho, A. C. Lima, I. S. Morais, and D. F. Santos, "Security challenges and recommendations in 5g-iot scenarios," in *International Conference on Advanced Information Networking and Applications*. Springer, 2023, pp. 558–573.

[95] A. Sinha, A. R. Thukkaraju, and O. Vyas, "A multi agent framework to detect in progress false data injection attacks for smart grid," in *International Conference on Advanced Network Technologies and Intelligent Computing*. Springer, 2021, pp. 123–141.

[96] K. Sonar and H. Upadhyay, "A survey: Ddos attack on internet of things," *International Journal of Engineering Research and Development*, vol. 10, no. 11, pp. 58–63, 2014.

[97] B. S. Rawal, S. Patel, and M. Sathiyanarayanan, "Identifying ddos attack using split-machine learning system in 5g and beyond networks," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2022, pp. 1–6.

[98] A. Munshi, N. A. Alqarni, and N. Abdullah Almalki, "Ddos attack on iot devices," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 2020, pp. 1–5.

[99] E. Džaferović, A. Sokol, A. Abd Almisreb, and S. M. Norzeli, "Dos and ddos vulnerability of iot: a review," *Sustainable Engineering and Innovation*, vol. 1, no. 1, pp. 43–48, 2019.

[100] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, p. 357430, 2014.

[101] C. R. GmbH. (2022) The nis 2 directive. [Online]. Available: https://www.nis-2-directive.com/

[102] K. Ganesh Kumar and S. Sengan, "Improved network traffic by attacking denial of service to protect resource using z-test based 4-tier geomark traceback (z4tgt)," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3541–3575, 2020.

[103] S. Hijazi and M. S. Obaidat, "Address resolution protocol spoofing attacks and security approaches: A survey," *Security and Privacy*, vol. 2, no. 1, p. e49, 2019.

[104] P. Madani, N. Vlajic, and S. Sadeghpour, "Mac-layer spoofing detection and prevention in iot systems: randomized moving target approach," in *Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy*, 2020, pp. 71–80.

[105] S. Murali and A. Jamalipour, "A lightweight intrusion detection for sybil attack under mobile rpl in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, 2019.

[106] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE communications surveys & tutorials*, vol. 21, no. 2, pp. 1636–1675, 2018.

[107] K. Ávila, P. Sanmartin, D. Jabba, and J. Gómez, "An analytical survey of attack scenario parameters on the techniques of attack mitigation in wsn," *Wireless Personal Communications*, pp. 1–32, 2022.

[108] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, "Passive rule-based approach to detect sinkhole attack in rpl-based internet of things networks," *IEEE Access*, 2023.

[109] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the internet of things from the layered context," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, p. e3935, 2022.

[110] C. Hong and D. Shi, "A cloud-based control system architecture for multi-uav," in *Proceedings of the 3rd International Conference on Robotics, Control and Automation*, 2018, pp. 25–30.

[111] M. K. Hooshmand and D. Hosahalli, "Network anomaly detection using deep learning techniques," *CAAI Transactions on Intelligence Technology*, vol. 7, no. 2, pp. 228–243, 2022.

[112] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect ddos attacks in blockchain-enabled iot network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, 2022.

[113] A. R. Wani, Q. Rana, U. Saxena, and N. Pandey, "Analysis and detection of ddos attacks on cloud computing environment using machine learning techniques," in *2019 Amity International conference on artificial intelligence (AICAI)*. IEEE, 2019, pp. 870–875.

[114] I. Baako and S. Umar, "An integrated vulnerability assessment of electronic commerce websites." *International Journal of Information Engineering & Electronic Business*, vol. 12, no. 5, 2020.

[115] A. Singh, A. Sharma, N. Sharma, I. Kaushik, and B. Bhushan, "Taxonomy of attacks on web based applications," in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1. IEEE, 2019, pp. 1231–1235.

[116] H. Ibrahim *et al.*, "A review on the mechanism mitigating and eliminating internet crimes using modern technologies: Mitigating internet crimes using modern technologies," *Wasit Journal of Computer and Mathematics Science*, vol. 1, no. 3, pp. 76–108, 2022.

[117] T. Hu, Z. Zhang, P. Yi, D. Liang, Z. Li, Q. Ren, Y. Hu, and J. Lan, "Seapp: A secure application management framework based on rest api access control in sdn-enabled cloud environment," *Journal of Parallel and Distributed Computing*, vol. 147, pp. 108–123, 2021.

[118] M. Kaur, M. Raj, and H.-N. Lee, "Cross channel scripting and code injection attacks on web and cloud-based applications: a comprehensive review," *Sensors*, vol. 22, no. 5, p. 1959, 2022.

[119] N. Krishnamoorthy and S. Umarani, "An experimental study on cloud computing security issues and a framework for xml ddos attack prevention," in *Journal of Physics: Conference Series*, vol. 2007, no. 1. IOP Publishing, 2021, p. 012058.

[120] U. K. Jannat and M. Mohankumar, "Proposed on attack analysis using risk assessment and security risk assessment using attacks for cloud cyber security," *Computer Science*, vol. 3, p. 1.

[121] R. Geetha, A. Suntheya, and G. U. Srikanth, "Cloud integrated iot enabled sensor network security: research issues and solutions," *Wireless Personal Communications*, vol. 113, pp. 747–771, 2020.

[122] R. Ponnumani and N. Partheeban, "Various threats and attack on cloud computing: A review," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE, 2022, pp. 1296–1300.

[123] M. Abbasi, M. Plaza-Hernández, J. Prieto, and J. M. Corchado, "Security in the internet of things application layer: Requirements, threats, and solutions," *IEEE Access*, vol. 10, pp. 97 197–97 216, 2022.

[124] S. Padmanaban, M. A. Nasab, M. E. Shiri, H. H. S. Javadi, M. A. Nasab, M. Zand, and T. Samavat, "The role of internet of things in smart homes," *Artificial Intelligence-based Smart Power Systems*, pp. 259–271, 2023.

[125] M. Kumar, C. Kondaiah, A. R. Pais, and R. S. Rao, "Machine learning models for phishing detection from tls traffic," *Cluster Computing*, pp. 1–15, 2023.

[126] A. Gaurav, B. B. Gupta, W. Alhalabi, A. Visvizi, and Y. Asiri, "A comprehensive survey on ddos attacks on various intelligent systems and it's defense techniques," *International Journal of Intelligent Systems*, vol. 37, no. 12, pp. 11 407–11 431, 2022.

[127] R. Ahuja and M. Gupta, "Improved heuristic framework for cyber security system on ddos attack," *Journal of Data Acquisition and Processing*, vol. 38, no. 3, p. 3033, 2023.

[128] F. Shaikh, E. Bou-Harb, N. Neshenko, A. P. Wright, and N. Ghani, "Internet of malicious things: Correlating active and passive measurements for inferring and characterizing internet-scale unsolicited iot devices," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 170–177, 2018.

[129] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, "Adopting internet of things for the development of smart buildings: A review of enabling technologies and applications," *Automation in Construction*, vol. 101, pp. 111–126, 2019.

[130] A. Shifa, M. N. Asghar, and M. Fleury, "Multimedia security perspectives in iot," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*. IEEE, 2016, pp. 550–555.

[131] . PwC. (2021) Conti cyber attack on the hse. [Online]. Available: https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

[132] M. S. Akhtar and T. Feng, "A systemic security and privacy review: Attacks and prevention mechanisms over iot layers," *EAI Endorsed Transactions on Security and Safety*, vol. 8, no. 30, 2022.

[133] M. A. Khatun, N. Chowdhury, and M. N. Uddin, "Malicious nodes detection based on artificial neural network in iot environments," in *2019 22nd International Conference on Computer and Information Technology (ICCIT)*. IEEE, 2019, pp. 1–6.

[134] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, "Ethical dilemmas and privacy issues in emerging technologies: a review," *Sensors*, vol. 23, no. 3, p. 1151, 2023.

[135] N. Comfort, "German banking regulator bafin's website hit by cyber attack," https://tinyurl.com/tmja7jyn, 2023, accessed: 15 October 2023.

[136] A. Raj, "Critical infrastructure cyberattack on japan's biggest port," https://tinyurl.com/2kn4mdxn, 2023, accessed: 15 October 2023.

[137] K. A. Nagaty, "Iot commercial and industrial applications and ai-powered iot," in *Frontiers of Quality Electronic Design (QED) AI, IoT and Hardware Security*. Springer, 2023, pp. 465–500.

[138] S. Gupta and B. B. Gupta, "Cross-site scripting (xss) attacks and defense mechanisms: classification and state-of-the-art," *International Journal of System Assurance Engineering and Management*, vol. 8, pp. 512–530, 2017.

[139] M. T. Louw and V. Venkatakrishnan, "Blueprint: Robust prevention of cross-site scripting attacks for existing browsers," in *2009 30th IEEE Symposium on Security and Privacy*, 2009, pp. 331–346.

[140] D. Lu, J. Fei, and L. Liu, "A semantic learning-based sql injection attack detection technology," *Electronics*, vol. 12, no. 6, p. 1344, 2023.

[141] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable artificial intelligence applications in cyber security: State-of-the-art in research," *IEEE Access*, 2022.

[142] S. M. Mathews, "Explainable artificial intelligence applications in nlp, biomedical, and malware classification: A literature review," in *Intelligent Computing: Proceedings of the 2019 Computing Conference, Volume 2*. Springer, 2019, pp. 1269–1292.

[143] M. R. Islam, M. U. Ahmed, S. Barua, and S. Begum, "A systematic review of explainable artificial intelligence in terms of different application domains and tasks," *Applied Sciences*, vol. 12, no. 3, p. 1353, 2022.

[144] H. H. Nguyen, F. Mirza, M. A. Naeem, and M. Nguyen, "A review on iot healthcare monitoring applications and a vision for transforming sensor data into real-time clinical feedback," in *2017 IEEE 21st international conference on computer supported cooperative work in design (CSCWD)*. IEEE, 2017, pp. 257–262.

[145] S. S. Ram, B. Apduhan, and N. Shiratori, "A machine learning framework for edge computing to improve prediction accuracy in mobile health monitoring," in *Computational Science and Its Applications–ICCSA 2019: 19th International Conference, Saint Petersburg, Russia, July 1–4, 2019, Proceedings, Part III 19*. Springer, 2019, pp. 417–431.

[146] P. Vanin, T. Newe, L. L. Dhirani, E. O'Connell, D. O'Shea, B. Lee, and M. Rao, "A study of network intrusion detection systems using artificial intelligence/machine learning," *Applied Sciences*, vol. 12, no. 22, p. 11752, 2022.

[147] L. L. Dhirani, T. Newe, and S. Nizamani, "Hybrid multi-cloud demystifying slas for smart city enterprises using iot applications," in *IoT Architectures, Models, and Platforms for Smart City Applications*. IGI Global, 2020, pp. 52–67.

[148] A. Sharma and U. K. Singh, "Modelling of smart risk assessment approach for cloud computing environment using ai & supervised machine learning algorithms," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 243–250, 2022.

[149] F. Desai, D. Chowdhury, R. Kaur, M. Peeters, R. C. Arya, G. S. Wander, S. S. Gill, and R. Buyya, "Healthcloud: A system for monitoring health status of heart patients using machine learning and cloud computing," *Internet of Things*, vol. 17, p. 100485, 2022.

[150] A. Abdelaziz, A. S. Salama, A. Riad, and A. N. Mahmoud, "A machine learning model for predicting of chronic kidney disease based internet of things and cloud computing in smart cities," *Security in smart cities: models, applications, and challenges*, pp. 93–114, 2019.

[151] C. Butpheng, K.-H. Yeh, and H. Xiong, "Security and privacy in iot-cloud-based e-health systems—a comprehensive review," *Symmetry*, vol. 12, no. 7, p. 1191, 2020.

[152] M. Maksimović and V. Vujović, "Internet of things based e-health systems: ideas, expectations and concerns," *Handbook of large-scale distributed computing in smart healthcare*, pp. 241–280, 2017.

[153] D. Zhang, J. J. P. C. Rodrigues, Y. Zhai, and T. Sato, "Design and implementation of 5g e-health systems: Technologies, use cases, and future challenges," *IEEE Communications Magazine*, vol. 59, no. 9, pp. 80–85, 2021.

[154] M. S. Hossain, S. U. Amin, M. Alsulaiman, and G. Muhammad, "Applying deep learning for epilepsy seizure detection and brain mapping visualization," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 15, no. 1s, pp. 1–17, 2019.

[155] C. Hewson, C. Vogel, and D. Laurent, *Internet research methods*. Sage, 2015.

[156] H. Asri, "Iot and reality mining for real-time disease prediction," in *IoT and Smart Devices for Sustainable Environment*. Springer, 2022, pp. 85–102.

[157] F. D. G. Solfa and F. R. Simonato, "Big data analytics in healthcare: Exploring the role of machine learning in predicting patient outcomes and improving healthcare delivery," *International Journal of Computations, Information and Manufacturing (IJCIM)*, vol. 3, no. 1, pp. 1–9, 2023.

[158] G. Arji, H. Ahmadi, P. Avazpoor, and M. Hemmat, "Identifying resilience strategies for disruption management in the healthcare supply chain during covid-19 by digital innovations: A systematic literature review," *Informatics in Medicine Unlocked*, p. 101199, 2023.

[159] L. L. Dhirani, T. Newe, and S. Nizamani, "Can iot escape cloud qos and cost pitfalls," in *2018 12th International Conference on Sensing Technology (ICST)*, 2018, pp. 65–70.

[160] H. Asri and Z. Jarir, "Toward a smart health: big data analytics and iot for real-time miscarriage prediction," *Journal of Big Data*, vol. 10, no. 1, pp. 1–23, 2023.

[161] G. Sasubilli and A. Kumar, "Machine learning and big data implementation on health care data," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2020, pp. 859–864.

[162] A. do Carmo Barriga, A. F. Martins, M. J. Simões, and D. Faustino, "The covid-19 pandemic: Yet another catalyst for governmental mass surveillance?" *Social Sciences & Humanities Open*, vol. 2, no. 1, p. 100096, 2020.

[163] S. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya, "End to end light weight mutual authentication scheme in iot-based healthcare environment," *Journal of Reliable Intelligent Environments*, vol. 6, pp. 3–13, 2020.

[164] E. Gelenbe and M. Nakip, "Real-time cyberattack detection with offline and online learning," in *2023 IEEE 29th International Symposium on*

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

Local and Metropolitan Area Networks (LANMAN). IEEE, 2023, pp. 1–6.

[165] P. A. Williams and V. McCauley, "Always connected: The security challenges of the healthcare internet of things," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. IEEE, 2016, pp. 30–35.

[166] M. Pons, E. Valenzuela, B. Rodríguez, J. A. Nolazco-Flores, and C. Del-Valle-Soto, "Utilization of 5g technologies in iot applications: Current limitations by interference and network optimization difficulties—a review," *Sensors*, vol. 23, no. 8, p. 3876, 2023.

[167] A. M. Seid, A. Erbad, H. N. Abishu, A. Albaseer, M. Abdallah, and M. Guizani, "Multi-agent federated reinforcement learning for resource allocation in uav-enabled internet of medical things networks," *IEEE Internet of Things Journal*, pp. 1–1, 2023.

[168] A. Rai, D. K. Singh, A. Sehgal, and K. Cengiz, *Paradigms of Smart and Intelligent Communication, 5G and Beyond*. Springer Nature, 2023.

[169] M. Vermanen, M. M. Rantanen, and V. Harkke, "Ethical framework for iot deployment in smes: individual perspective," *Internet Research*, vol. 32, no. 7, pp. 185–201, 2022.

[170] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "Iot cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP Journal on Information Security*, vol. 2020, no. 1, pp. 1–18, 2020.

[171] A. Karale, "The challenges of iot addressing security, ethics, privacy, and laws," *Internet of Things*, vol. 15, p. 100420, 2021.

[172] L. Phillips, "Healthcare cybersecurity in 2023: Hive's shutdown is good news but cyberattacks are only getting worse," *Insider Intelligence*, 2023. [Online]. Available: https://tinyurl.com/mryu9yct

[173] J. McKeon, "Biggest healthcare data breaches reported this year, so far," 2023. [Online]. Available: https://tinyurl.com/2s3t6dmh

[174] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[175] J. Qiu, X. Liang, S. Shetty, and D. Bowden, "Towards secure and smart healthcare in smart cities using blockchain," in *2018 IEEE International Smart Cities Conference (ISC2)*, 2018, pp. 1–4.

[176] I. Raeesi Vanani and M. Amirhosseini, "Iot-based diseases prediction and diagnosis system for healthcare," *Internet of Things for Healthcare Technologies*, pp. 21–48, 2021.

[177] A. W. Kempa-Liehr, C. Y.-C. Lin, R. Britten, D. Armstrong, J. Wallace, D. Mordaunt, and M. O'Sullivan, "Healthcare pathway discovery and probabilistic machine learning," *International journal of medical informatics*, vol. 137, p. 104087, 2020.

[178] A. U. Haq, J. P. Li, J. Khan, M. H. Memon, S. Nazir, S. Ahmad, G. A. Khan, and A. Ali, "Intelligent machine learning approach for effective recognition of diabetes in e-healthcare using clinical data," *Sensors*, vol. 20, no. 9, p. 2649, 2020.

[179] R. Vaishya, M. Javaid, I. H. Khan, and A. Haleem, "Artificial intelligence (ai) applications for covid-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp. 337–339, 2020.

[180] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, vol. 121, p. 102583, 2023.

[181] A. J. Cartwright, "The elephant in the room: cybersecurity in healthcare," *Journal of Clinical Monitoring and Computing*, pp. 1–10, 2023.

[182] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends," *Cyber Security and Applications*, p. 100016, 2023.

[183] M. Kumar, A. Kumar, S. Verma, P. Bhattacharya, D. Ghimire, S.-h. Kim, and A. S. Hosen, "Healthcare internet of things (h-iot): Current trends, future prospects, applications, challenges, and security issues," *Electronics*, vol. 12, no. 9, p. 2050, 2023.

[184] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for iot attacks using deep learning technique," *Computers and Electrical Engineering*, vol. 107, p. 108626, 2023.

[185] M. Khatkar, K. Kumar, B. Kumar, and P. Agarwal, "Parametric influence of intrusion detection system in healthcare sector using deep neural [lstm] network," *Journal of Pharmaceutical Negative Results*, pp. 685–692, 2023.

[186] S. Ksibi, F. Jaidi, and A. Bouhoula, "Iomt security model based on machine learning and risk assessment techniques," in *2023 International Wireless Communications and Mobile Computing (IWCMC)*, 2023, pp. 614–619.

[187] K. Bouabida, B. Lebouché, and M.-P. Pomey, "Telehealth and covid-19 pandemic: an overview of the telehealth use, advantages, challenges, and opportunities during covid-19 pandemic," in *Healthcare*, vol. 10, no. 11. MDPI, 2022, p. 2293.

[188] L. Wang and R. Jones, "Big data, cybersecurity, and challenges in healthcare," in *2019 SoutheastCon*, 2019, pp. 1–6.

[189] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[190] S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, "A fuzzy-based duo-secure multi-modal framework for iomt anomaly detection," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 131–144, 2023.

[191] T. Thulasi and K. Sivamohan, "Lso-csl: Light spectrum optimizer-based convolutional stacked long short term memory for attack detection in iot-based healthcare applications," *Expert Systems with Applications*, vol. 232, p. 120772, 2023.

[192] K. Gupta, D. K. Sharma, K. D. Gupta, and A. Kumar, "A tree classifier based network intrusion detection model for internet of medical things," *Computers and Electrical Engineering*, vol. 102, p. 108158, 2022.

[193] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," *IEEE Access*, vol. 8, pp. 106 576–106 584, 2020.

[194] S. Saif, P. Das, S. Biswas, M. Khari, and V. Shanmuganathan, "Hiids: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in iot based healthcare," *Microprocessors and Microsystems*, p. 104622, 2022.

[195] S. Ray, K. N. Mishra, and S. Dutta, "Detection and prevention of ddos attacks on m-healthcare sensitive data: a novel approach," *International Journal of Information Technology*, vol. 14, no. 3, pp. 1333–1341, 2022.

[196] A. Kumar, R. S. Umurzoqovich, N. D. Duong, P. Kanani, A. Kuppusamy, M. Praneesh, and M. N. Hieu, "An intrusion identification and prevention for cloud computing: From the perspective of deep learning," *Optik*, vol. 270, p. 170044, 2022.

[197] S. P. RM, P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for dnn using hybrid pca-gwo for intrusion detection in iomt architecture," *Computer Communications*, vol. 160, pp. 139–149, 2020.

[198] S. O. M. Kamel and S. A. Elhamayed, "Mitigating the impact of iot routing attacks on power consumption in iot healthcare environment using convolutional neural network," *International Journal of Computer Network and Information Security*, vol. 12, no. 4, pp. 11–29, 2020.

[199] N. Terry, "Existential challenges for healthcare data protection in the united states," *Ethics, Medicine and Public Health*, vol. 3, no. 1, pp. 19–27, 2017.

[200] M. Bansal *et al.*, "Application layer protocols for internet of healthcare things (ioht)," in *2020 fourth international conference on inventive systems and control (ICISC)*. IEEE, 2020, pp. 369–376.

[201] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of things (iot): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 474–10 498, 2021.

[202] B. Mittelstadt, "Designing the health-related internet of things: ethical principles and guidelines," *Information*, vol. 8, no. 3, p. 77, 2017.

[203] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, "A systematic literature review on machine and deep learning approaches for detecting attacks in rpl-based 6lowpan of internet of things," *Sensors*, vol. 22, no. 9, p. 3400, 2022.

[204] R. SAMINATHAN, S. SARAVANAN, and P. ANBALAGAN, "Blockchain in healthcare: A new dimension to healthcare data security," *Hybridization of Blockchain and Cloud Computing: Overcoming Security Issues in IoT*, p. 45, 2023.

[205] B. H. Patel and P. Shah, "Rpl routing protocol performance under sinkhole and selective forwarding attack: experimental and simulated evaluation," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, pp. 1849–1856, 2020.

[206] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1910–1923, 2017.

[207] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "Iot smart health security threats," in *2019 19th International conference on computational science and its applications (ICCSA)*. IEEE, 2019, pp. 26–31.

[208] F. Zahra, N. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M. A. AlZain, "Rank and wormhole attack detection model for rpl-based internet of things using machine learning," *Sensors*, vol. 22, no. 18, p. 6765, 2022.

[209] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review," *Sensors*, vol. 23, no. 8, p. 4117, 2023.

[210] A. Haghrah, M. P. Abdollahi, H. Azarhava, and J. M. Niya, "A survey on the handover management in 5g-nr cellular networks: aspects, approaches and challenges," *EURASIP Journal on Wireless Communications and Networking*, vol. 2023, no. 1, pp. 1–57, 2023.

[211] T. M. Ghazal, "Positioning of uav base stations using 5g and beyond networks for iomt applications," 2021.

[212] A. Peivandizadeh and B. Molavi, "Compatible authentication and key agreement protocol for low power and lossy network in iot environment." *Available at SSRN 4454407*, 2023.

[213] Y. Rbah, M. Mahfoudi, Y. Balboul, M. Fattah, S. Mazer, M. Elbekkali, and B. Bernoussi, "Machine learning and deep learning methods for intrusion detection systems in iomt: A survey," in *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, 2022, pp. 1–9.

[214] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An efficient cnn-based deep learning model to detect malware attacks (cnn-dma) in 5g-iot healthcare applications," *Sensors*, vol. 21, no. 19, p. 6346, 2021.

[215] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—a review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 527–555, 2022.

[216] P. N. Mahalle, G. R. Shinde, Y. S. Ingle, and N. N. Wasatkar, "Data-centric ai in information, communication and technology," in *Data Centric Artificial Intelligence: A Beginner's Guide*. Springer, 2023, pp. 109–124.

[217] I. N. R. Hendrawan and I. G. N. W. Arsa, "Zolertia z1 energy usage simulation with cooja simulator," in *2017 1st International Conference on Informatics and Computational Sciences (ICICoS)*, 2017, pp. 147–152.

[218] E. Q. Shahra, T. R. Sheltami, and E. M. Shakshuki, "A comparative study of range-free and range-based localization protocols for wireless sensor network: Using cooja simulator," in *Sensor technology: Concepts, methodologies, tools, and applications*. IGI Global, 2020, pp. 1522–1537.

[219] Q. Wang, Y. Ma, K. Zhao, and Y. Tian, "A comprehensive survey of loss functions in machine learning," *Annals of Data Science*, pp. 1–26, 2020.

[220] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN computer science*, vol. 2, no. 3, p. 160, 2021.

[221] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 524–552, 2020.

[222] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 112 392–112 415, 2022.

[223] T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam, "Analysis of iot security challenges and its solutions using artificial intelligence," *Brain Sciences*, vol. 13, no. 4, p. 683, 2023.

[224] I. H. Sarker, "Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects," *Annals of Data Science*, pp. 1–26, 2022.

[225] ——, "Cyberlearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," *Internet of Things*, vol. 14, p. 100393, 2021.

[226] D. Alahakoon, R. Nawaratne, Y. Xu, D. De Silva, U. Sivarajah, and B. Gupta, "Self-building artificial intelligence and machine learning to empower big data analytics in smart cities," *Information Systems Frontiers*, pp. 1–20, 2020.

[227] K. Kumar and B. P. Pande, "Applications of machine learning techniques in the realm of cybersecurity," *Cyber Security and Digital Forensics*, pp. 295–315, 2022.

[228] V. Ravi, T. D. Pham, and M. Alazab, "Attention-based multidimensional deep learning approach for cross-architecture iomt malware detection and classification in healthcare cyber-physical systems," *IEEE Transactions on Computational Social Systems*, 2022.

[229] A. Singla and E. Bertino, "How deep learning is making information security more intelligent," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 56–65, 2019.

[230] S. Roobini, M. Kavitha, M. Sujaritha, and D. R. Kumar, "Cyber-security threats to iomt-enabled healthcare systems," in *Cognitive Computing for Internet of Medical Things*. Chapman and Hall/CRC, 2022, pp. 105–130.

[231] Q. Qiao and A. Yunusa-Kaltungo, "A hybrid agent-based machine learning method for human-centred energy consumption prediction," *Energy and Buildings*, vol. 283, p. 112797, 2023.

[232] B. Sharma, L. Sharma, and C. Lal, "Feature selection and deep learning technique for intrusion detection system in iot," in *Proceedings of International Conference on Computational Intelligence: ICCI 2020*. Springer, 2022, pp. 253–261.

[233] P. R. S. Rohith and H. Rathore, "Sentiment analysis of imdb movie reviews: A comparative analysis of feature selection and feature extraction techniques," in *Hybrid Intelligent Systems: 21st International Conference on Hybrid Intelligent Systems (HIS 2021), December 14–16, 2021*, vol. 420. Springer Nature, 2022, p. 283.

[234] A. Z. Ul-Saufie, N. H. Hamzan, Z. Zahari, W. N. Shaziayani, N. M. Noor, M. R. R. M. A. Zainol, A. V. Sandu, G. Deak, and P. Vizureanu, "Improving air pollution prediction modelling using wrapper feature selection," *Sustainability*, vol. 14, no. 18, p. 11403, 2022.

[235] Doreswamy, M. K. Hooshmand, and I. Gad, "Feature selection approach using ensemble learning for network anomaly detection," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 4, pp. 283–293, 2020.

[236] D. He, Q. Qiao, Y. Gao, J. Zheng, S. Chan, J. Li, and N. Guizani, "Intrusion detection based on stacked autoencoder for connected healthcare systems," *IEEE Network*, vol. 33, no. 6, pp. 64–69, 2019.

[237] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, "Survey of machine learning based intrusion detection methods for internet of medical things," *Applied Soft Computing*, p. 110227, 2023.

[238] O. Taouali, S. Bacha, K. Ben Abdellafou, A. Aljuhani, K. Zidi, R. Alanazi, and M. F. Harkat, "Intelligent intrusion detection system for the internet of medical things based on data-driven techniques." *Computer Systems Science & Engineering*, vol. 47, no. 2, 2023.

[239] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for internet of medical things," *IEEE Access*, vol. 8, pp. 181 560–181 576, 2020.

[240] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," *Computer Communications*, vol. 166, pp. 110–124, 2021.

[241] A. A. Abdellatif, A. Mohamed, C. F. Chiasserini, M. Tlili, and A. Erbad, "Edge computing for smart health: Context-aware approaches, opportunities, and challenges," *IEEE Network*, vol. 33, no. 3, pp. 196–203, 2019.

[242] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014.

[243] A. Ukil, S. Bandyoapdhyay, C. Puri, and A. Pal, "Iot healthcare analytics: The importance of anomaly detection," in *2016 IEEE 30th international conference on advanced information networking and applications (AINA)*. IEEE, 2016, pp. 994–997.

[244] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017, pp. 3648–3656.

[245] A. Mehra, M. Mandal, P. Narang, and V. Chamola, "Correction to "reviewnet: A fast and resource optimized network for enabling safe autonomous driving in hazy weather conditions"[jul 21 4256-4266]," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2888–2888, 2022.

[246] R. A. Mohammed and K. M. A. Alheeti, "Intrusion detection system for healthcare based on convolutional neural networks," in *2022 Iraqi International Conference on Communication and Information Technologies (IICCIT)*. IEEE, 2022, pp. 216–221.

[247] D. Gil, M. Johnsson, H. Mora, and J. Szymański, "Review of the complexity of managing big data of the internet of things," *Complexity*, vol. 2019, 2019.

[248] L. Datta, "A survey on activation functions and their relation with xavier and he normal initialization," *arXiv preprint arXiv:2004.06632*, 2020.

[249] V. Andrearczyk and P. F. Whelan, "Convolutional neural network on three orthogonal planes for dynamic texture classification," *Pattern Recognition*, vol. 76, pp. 36–49, 2018.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3346320

[250] V. Sze, Y.-H. Chen, T.-J. Yang, and J. S. Emer, "Efficient processing of deep neural networks: A tutorial and survey," *Proceedings of the IEEE*, vol. 105, no. 12, pp. 2295–2329, 2017.

[251] K. Khalil, O. Eldash, A. Kumar, and M. Bayoumi, "Designing novel aad pooling in hardware for a convolutional neural network accelerator," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 3, pp. 303–314, 2022.

[252] R. Nirthika, S. Manivannan, A. Ramanan, and R. Wang, "Pooling in convolutional neural networks for medical image analysis: a survey and an empirical study," *Neural Computing and Applications*, vol. 34, no. 7, pp. 5321–5347, 2022.

[253] A. Sharma, S. Rani, S. H. Shah, R. Sharma, F. Yu, and M. M. Hassan, "An efficient hybrid deep learning model for denial of service detection in cyber physical systems," *IEEE Transactions on Network Science and Engineering*, 2023.

[254] N. Faruqui, M. A. Yousuf, M. Whaiduzzaman, A. Azad, S. A. Alyami, P. Liò, M. A. Kabir, and M. A. Moni, "Safetymed: A novel iomt intrusion detection system using cnn-lstm hybridization," *Electronics*, vol. 12, no. 17, p. 3541, 2023.

[255] M. Hasan *et al.*, "Attack and anomaly detection in iot sensors in iot sites using machine learning approaches. internet of things 7 (2019)," 2019.

[256] R. Patgiri, H. Katari, R. Kumar, and D. Sharma, "Empirical study on malicious url detection using machine learning," in *Distributed Computing and Internet Technology: 15th International Conference, ICDCIT 2019, Bhubaneswar, India, January 10–13, 2019, Proceedings 15*. Springer, 2019, pp. 380–388.

[257] J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong, "Anomaly detection in internet of medical things with blockchain from the perspective of deep neural network," *Information Sciences*, vol. 617, pp. 133–149, 2022.

[258] S. Chaudhary, R. Kakkar, N. K. Jadav, A. Nair, R. Gupta, S. Tanwar, S. Agrawal, M. D. Alshehri, R. Sharma, G. Sharma *et al.*, "A taxonomy on smart healthcare technologies: security framework, case study, and future directions," *Journal of Sensors*, vol. 2022, 2022.

[259] S. Rajendran, R. K. Panneerselvam, P. J. Kumar, V. A. Rajasekaran, P. Suganya, S. K. Mathivanan, and P. Jayagopal, "Prescreening and triage of covid-19 patients through chest x-ray images using deep learning model," *Big Data*, 2022.

[260] Z. Hau and E. C. Lupu, "Exploiting correlations to detect false data injections in low-density wireless sensor networks," in *Proceedings of the 5th on Cyber-Physical System Security Workshop*, 2019, pp. 1–12.

[261] M. Begli, F. Derakhshan, and H. Karimipour, "A layered intrusion detection system for critical infrastructure using machine learning," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, 2019, pp. 120–124.

[262] S. Sengan, O. I. Khalaf, D. K. Sharma, A. A. Hamad *et al.*, "Secured and privacy-based ids for healthcare systems on e-medical data using machine learning approach," *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, vol. 11, no. 3, pp. 1–11, 2022.

[263] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare internet of things: A survey of emerging technologies," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[264] R. Sharma, "Software-defined networking for healthcare internet of things," in *Applications of Machine Learning in Big-Data Analytics and Cloud Computing*. River Publishers, 2022, pp. 231–247.

[265] P. Ajmani and P. Saigal, "5g and iot for smart farming," in *Applying Drone Technologies and Robotics for Agricultural Sustainability*. IGI Global, 2023, pp. 124–139.

[266] D. Gowda, A. Sharma, B. K. Rao, R. Shankar, P. Sarma, A. Chaturvedi, and N. Hussain, "Industrial quality healthcare services using internet of things and fog computing approach," *Measurement: Sensors*, vol. 24, p. 100517, 2022.

[267] S. Sutradhar, S. Karforma, R. Bose, and S. Roy, "A dynamic step-wise tiny encryption algorithm with fruit fly optimization for quality of service improvement in healthcare," *Healthcare Analytics*, vol. 3, p. 100177, 2023.

[268] M. Adil, J. Ali, M. M. Jadoon, S. R. Alotaibi, N. Kumar, A. Farouk, and H. Song, "Covid-19: Secure healthcare internet of things networks, current trends and challenges with future research directions," *ACM Transactions on Sensor Networks*, vol. 19, no. 3, pp. 1–25, 2023.

[269] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future iot-driven healthcare 4.0 technologies: A survey, current challenges and future directions," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 1, pp. 361–407, 2023.

[270] F. Sallabi, F. Naeem, M. Awad, and K. Shuaib, "Managing iot-based smart healthcare systems traffic with software defined networks," in *2018 international symposium on networks, computers and communications (ISNCC)*. IEEE, 2018, pp. 1–6.

[271] J. H. Abawajy and M. M. Hassan, "Federated internet of things and cloud computing pervasive patient health monitoring system," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 48–53, 2017.

[272] R. Taheri, H. Ahmed, and E. Arslan, "Deep learning for the security of software-defined networks: a review," *Cluster Computing*, vol. 26, no. 5, pp. 3089–3112, 2023.

[273] H. Elubeyd and D. Yiltas-Kaplan, "Hybrid deep learning approach for automatic dos/ddos attacks detection in software-defined networks," *Applied Sciences*, vol. 13, no. 6, p. 3828, 2023.

[274] M. Cicioğlu and A. Çalhan, "A multiprotocol controller deployment in sdn-based iomt architecture," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 20 833–20 840, 2022.

[275] V. Lakshminarayanan, A. Ravikumar, H. Sriraman, S. Alla, and V. K. Chattu, "Health care equity through intelligent edge computing and augmented reality/virtual reality: A systematic review," *Journal of Multidisciplinary Healthcare*, pp. 2839–2859, 2023.

[276] A. S. Ahmed and H. A. Salah, "Development a software defined network (sdn) with internet of things (iot) security for medical issues conti cyber attack," *Journal of Al-Qadisiyah for computer science and mathematics*, vol. 15, no. 3, pp. Page–98, 2023.

MIRZA AKHI KHATUN (MEMBER, IEEE) is currently pursuing the Ph.D. degree at the Department of Electronic and Computer Engineering, University of Limerick, Ireland. She earned an MSc in Computer Science and Engineering from Jagannath University, Bangladesh, with a focus on Internet of Things (IoT) security and Machine Learning (ML). Her ongoing research delves into healthcare IoT security, utilizing AI/ML innovations. She has an exemplary academic background in computer science. Notably, she was awarded a scholarship from the Science Foundation Ireland Centre for Research Training in Foundations of Data Science (2022). During her Master of Science program, she secured the first position in her class. The author has also published research papers at renowned IEEE international conferences and is an active member of the IEEE, reflecting her deep commitment to the professional community. Her research interests span IoT, Artificial Intelligence, Machine Learning, Data Analysis, Network Security, and Systems Architecture.

DR. SANOBER FARHEEN MEMON (MEMBER IEEE) is a Researcher on the OXI-SMART Project at the Optical Fibre Sensors Research Centre, Department of Electronic and Computer Engineering (ECE), University of Limerick (UL), Ireland. Sanober received a B.Eng Degree in Electronic Engineering and an M.Eng Degree in Electronic Systems Engineering from Mehran University of Engineering & Technology (MUET) Jamshoro, Pakistan in 2010 and 2014, respectively. She received her Ph.D. degree in Electronic and Computer Engineering from the University of Limerick, Ireland in 2023. During her doctoral research, she developed plastic optical fibre sensors for in-situ and real-time ultra low-level ethanol concentration measurement in microalgal bioethanol production applications. Sanober also served MUET, Pakistan for more than 3 years as a faculty member (Lecturer and Visiting Lecturer) and taught a variety of modules to B.Eng. students. Her current research interests include optical fibre sensors, medical sensors, photonics engineering, instrumentation and measurement, and intelligent systems. Sanober has been a recipient of multiple funding grants including the European Union EM INTACT Doctorate Scholarship, UL Postgraduate Residential Scholarship, UL Funding & ECE Departmental Funding, Merit Scholarship from MUET, Pakistan and some international travel/conference participation grants. She is a member of IEEE WIE, IEEE Photonics Society, IEEE Instrumentation & Measurement Society and SPIE.

CIARÁN EISING (SENIOR MEMBER, IEEE) received the BE in Electronic and Computer Engineering and a PhD from the NUI Galway, in 2003 and 2010, respectively. From 2009 to 2020, he was a Computer Vision Team Lead, Architect, and Senior Expert with Valeo. In 2020, he joined the University of Limerick as an Associate Professor of AI and Computer Vision.

DR. LUBNA LUXMI DHIRANI is an Assistant Professor at Department of Electronic & Computer Engineering, University of Limerick. She is the Course Director for the BSc Cybersecurity Practitioner Apprenticeship program. Lubna is a Senior Member IEEE, the first WIE Ambassador from Ireland in the IEEE WIE (UK&I section) and member of National Standards Authority of Ireland (NSAI). Lubna did her Ph.D. in Hybrid Cloud Computing QoS and SLA-based issues in Heterogenous Cloud Environment, MSc in Business Information Technology and B.Eng in Computer Systems. Lubna's has worked on interdisciplinary, industry-based projects securing machine-to-machine communications in Industry 4.0, V2I Safety and Security, Digital healthcare, etc. Her research interests include: cybersecurity, privacy, data governance, risk, cyber law, regulations, IIoT, IT/OT, cloud and security standards. Lubna's publications are listed at: Lubna Luxmi Dhirani - Google Scholar, she has delivered more than 35 technical workshops, tutorials, masterclasses, panel and keynote speeches at International Conferences and Platforms.

• • •